Securitas

Risk Intelligence Center

Estimación anual de inteligencia

Estimación para 2026

Enero de 2026

intelligence@securitas.com

Contenido

Introducción

Mike Evans

Director, Risk Intelligence Center

UN MUNDO NUEVO Y VALIENTE: DONDE HAY RIESGO, HAY OPORTUNIDAD

Nunca antes ha existido un momento y un lugar donde tanto la Seguridad como el Riesgo deben ir más allá, más rápido y estar mejor preparados para el futuro, para proteger a las organizaciones. La seguridad no es un 'centro de costos', es un facilitador estratégico para 'hacer negocios', y el riesgo no es un medio para gestionar ese 'coste', es una capacidad para la toma de decisiones. La Seguridad y el Riesgo, cuando se impulsan como parte de una estrategia liderada por la Inteligencia, proporcionan a las organizaciones la ventaja y la confianza necesarias para gestionar el riesgo y aprovechar oportunidades.

Los acontecimientos en los últimos días de 2025 — en el primero de 2026— marcan el rumbo del panorama de Riesgo y Seguridad para el próximo año:

- **Poco probable no significa imposible:** (Re) ver los riesgos de baja probabilidad y alto impacto como una cuestión de "¿cuándo, no si?" y prepararse para los peores escenarios ayuda a lograr los mejores resultados posibles.

- **La divergencia impulsa la convergencia:** El mundo está cambiando. Las organizaciones están siendo afectadas directa (e indirectamente) por eventos globales y locales, tanto física como digitalmente, sean conscientes o no, y la conciencia y comprensión de la situación son clave para una respuesta eficaz.

- **La seguridad es un facilitador estratégico:** Donde hay riesgo, hay oportunidad, y con la apertura (y cierre de nuevos mercados), el cambio en el apetito de los consumidores y el sentimiento público, la Seguridad y el Riesgo son esenciales para proteger a las organizaciones y permitirles alcanzar sus objetivos.

Desde la perspectiva de un tomador de decisiones, el clima actual suele considerarse 'Alto Riesgo / Alta Recompensa'. Sin embargo, otra forma de ver esto es 'Riesgo gestionado / Máxima Recompensa', un tema clave para las organizaciones en el incierto panorama global de riesgo actual, y fundamental para la Estimación Anual de Inteligencia 2026 del Securitas Risk Intelligence Center (RIC).

¿CUÁL ES LA ESTIMACIÓN ANUAL DE INTELIGENCIA DEL RIC DE SECURITAS?

La Estimación Anual de Inteligencia del Centro de Inteligencia de Riesgos de Securitas (RIC) proporciona inteligencia accionable para profesionales de la seguridad corporativa y los riesgos de seguridad para el año que viene – y más allá.

La Estimación Anual de Inteligencia incluye:

- **Análisis de seguridad estratégica y factores de riesgo:** identificar temas clave, tendencias, patrones y señales emergentes que moldean el panorama de seguridad y riesgo en 2026.

- **Inteligencia de seguridad corporativa:** aplicable a las evaluaciones organizaciones de todos los sectores y ubicaciones, incluyendo análisis de amenazas e inteligencia protectora.

- **Evaluaciones de Inteligencia de Riesgos Globales:** cubre preocupaciones de inteligencia panorama de Riesgo y Seguridad para el próximo año: globales, regionales y locales, incluyendo análisis de amenazas y riesgos geopolíticos.

- **Análisis de escenarios:** comodines que exploran una selección de escenarios de alto impacto y baja probabilidad con implicaciones de gran alcance para las organizaciones.

- **Fechas clave en 2026** que destacan los puntos críticos de mayor amenaza y riesgos asociados a eventos programados, incluidos eventos geopolíticos, políticos y sociales.

El informe pretende ser una alternativa accionable a otras evaluaciones temáticas, teniendo en cuenta a los responsables de la toma de decisiones en seguridad. La Estimación Anual de Inteligencia sirve de puente entre las evaluaciones estratégicas de riesgos destinadas a una audiencia ejecutiva y el análisis táctico destinado a la primera línea, para apoyar a quienes son responsables de proteger a su gente, propiedades y todo lo que más importe.

La Estimación Anual de Inteligencia proporciona conciencia situacional y comprensión para organizaciones de todos los sectores e industrias, y como tal se elabora como un resumen de alto nivel digerible para un público general, completo con consideraciones prácticas. El RIC también produce evaluaciones específicas de la organización, relevantes para el sector y adaptadas geográficamente, que están disponibles bajo solicitud.

Si tiene alguna pregunta sobre este informe, o si desea discutir sus requisitos específicos de inteligencia, por favor contáctese con el RIC.

Nuestro kit de herramientas de inteligencia

Concientización

Informes regulares programados y Ad Hoc sobre el panorama global de seguridad y amenazas. Incluyendo informes de inteligencia (INTREPs) e informes de situación (SITREPs):

- Informes diarios de Inteligencia Global.
- Perspectivas semanales de Inteligencia Global.
- Previsiones mensuales de amenazas.
- Resúmenes mensuales de Inteligencia (INTSUMs).
- Reportes de situaciones (SITREPs) e Informes de Inteligencia (INTREPs) para desarrollos significativos.

Alertas

Alertas por correo electrónico geodirigidas para eventos de una solución integral de Inteligencia de Protección, Amenazas y Riesgos para tu organización, operaciones y marca. Incluye: seguridad y amenazas cercanas. Totalmente personalizable según la gravedad, proximidad y frecuencia según los tipos de incidentes:

- Criminalidad.
- Orden Público.
- Terrorismo.
- Clima.
- Viajes y transporte.

Recomendaciones

Una solución integral de Inteligencia de Protección, Amenazas y Riesgos para tu organización, operaciones y marca. Incluye:

- Seguimiento de tus necesidades específicas.
- Seguimiento diario, resúmenes de inteligencia.
- Informes inmediatos para advertencias, inteligencia.
- Solución de amenazas, protección y riesgos.
- Acceso al servicio de informes ad hoc bajo demanda.

Analistas

Recursos dedicados a la inteligencia junto con la experiencia de Securitas en la comunidad global de Inteligencia.

Equipados con todas las herramientas y el entrenamiento necesario para apoyar tus necesidades de inteligencia y proteger tu organización.

Inteligencia Ad Hoc

Experiencia y consultoría en la materia para cualquier requisito de inteligencia dinámico específico.
Los tipos de informes comunes incluyen, pero no se limitan a:

- Informe de seguridad de viajes y viajeros: análisis en profundidad de las amenazas a la seguridad y protección en los viajes.
- Protección ejecutiva y evaluación defensiva: evaluación de vulnerabilidad de la información de un principal objetivo (es decir, un ejecutivo).
- Evaluaciones y filtros de seguridad de eventos: diligencia debida y monitorización en vivo.

Conoce al equipo


ALEX JOHNSON


ALMA ABRAHAM


ANASTASIA JOBARD


BEN GIDDINGS


CIAN LYNCH


FREDDIE VENABLES


JOHN COUDRIET


JOSHUA MENDELSON


JUANITA JOHNSON


KIMBERLEY DEAN


LAURA STEVENS


LOUISE MARTIN


LUCY DICKENS


MATT PHILLIPS

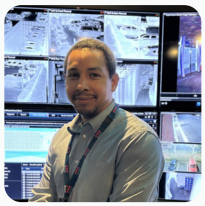

NATHAN SKEET


NICK FULLICK


OLIVER BACCHUS


SOPHIE CAIRNEY


CHARMIAN TAYLOR


PIERS REGISTER


ALEX BLITZ


JESS WILSON


JOE BECKFORD


OZICHI EGEONU


MIKE EVANS

Enfoque

El RIC emplea una estrategia de inteligencia de fuentes múltiples, utilizando todas las fuentes disponibles y apropiadas según el(los) requerimiento(s) de inteligencia.

Este enfoque combina la experiencia de nuestros analistas internos, la red global de la organización Securitas, terceros y socios, y tecnología de vanguardia para inteligencia de fuentes abiertas (OSINT), para producir la inteligencia final de la más alta calidad. La inclusión de información en la Estimación Anual de Inteligencia no es una afirmación de que alguno de estos escenarios ocurrirá, sino que existe el potencial de que la amenaza se manifieste y que la amenaza debe considerarse al realizar revisiones de seguridad y evaluaciones de riesgos.

Niveles de amenaza

Este informe utiliza el sistema de niveles de amenaza del RIC para puntuar las amenazas en una escala del 1 al 5 según la probabilidad y gravedad evaluadas, o la intención y capacidad.

5 - EXTREMO	Nivel de amenaza extrema/disrupción. Revise y responda de ser necesario.
4 - ALTO	Nivel de disrupción alto. Considere tomar acciones apropiadas.
3 - MODERADO	Amenaza moderada. Mantenga la alerta, y considere precauciones.
2 - BAJO	Amenaza baja / limitada. Esté alerta.
1 - MUY BAJO	Nivel de disrupción insignificante. Esté alerta.

Lenguaje de la probabilidad

Este informe utiliza el lenguaje de probabilidad del RIC para evaluar la probabilidad de que una amenaza se manifieste, eexpresándola mediante porcentajes, fracciones o proporciones como base de referencia. Esto ayuda a proporcionar contexto y claridad, y favorece una comprensión estandarizada de la evaluación y los términos utilizados.

Término	Probabilidad
Remoto	0-5%
Altamente improbable	10-20%
Improbable	25-35%
Posible	40-50%
Probable	55-75%
Altamente probable	80-90%
Casi cierto	95-99%

Fecha de corte de inteligencia	**0000hrs UTC 05 de enero de 2026**

Tendencias, patrones y factores influentes

Las Estimaciones Anuales de Inteligencia de la RIC de 2023, 2024 y 2025 notaron una variedad de tendencias y patrones dentro del panorama global de amenazas a la seguridad, todas ellas con impactos directos en las organizaciones, incluyendo su seguridad, operaciones, marca y reputación. Algunas de estas amenazas se han superpuesto en los últimos años, avanzando y evolucionando hasta incorporar a nuevos actores de riesgo, tácticas y objetivos completamente nuevos que también han sido puestos en primer plano. Las organizaciones se han enfrentado cada vez más a amenazas crecientes y riesgos incrementados como resultado de la evolución del panorama global de amenazas, lo que refuerza aún más la necesidad de inteligencia proactiva para informar a las organizaciones sobre las amenazas más urgentes. Los escenarios de amenaza/riesgo de seguridad corporativa incluidos en las Estimaciones Anuales de Inteligencia del RIC de 2023, 2024, 2025 y 2026 tienen como objetivo proporcionar a las organizaciones con una ventaja de toma de decisiones para limitar los posibles impactos del panorama global de amenazas, con los principales temas que se describen a continuación:

2023

- Las iniciativas ASG provocan reacciones adversas y amenazas a la seguridad
- Las presiones crónicas del cambio climático y los impactos repentinos de los desastres naturales
- Equilibrando la seguridad sanitaria frente a la hipersensibilidad
- El panorama de amenazas cibernéticas en constante evolución
- Desorden informativo y la creciente amenaza real de las noticias falsas
- El panorama activista en expansión
- (R)evolución en el terrorismo y el extremismo
- Espionaje dirigido a organizaciones y sus activos
- Resiliencia energética y seguridad
- Amenazas a la resiliencia y seguridad de la cadena de suministro global

2024

- Convergencia de las motivaciones de los actores de amenazas geopolíticas y sociopolíticas
- Los puntos de estrangulamiento y la competencia entre grandes potencias interrumpen las cadenas de suministro
- Superciclo electoral en 2024
- Carrera armamentística de inteligencia artificial
- Los riesgos climáticos y medioambientales alcanzan nuevos límites
- Ciberdelitos potenciados
- Impactos globales de la recesión económica de China
- La reacción contra el ASG pasa de las palabras a los hechos
- La infraestructura crítica seguirá siendo una vulnerabilidad crítica
- El aumento del espionaje corporativo desplaza el enfoque hacia la contrainteligencia

2025

- El cambio de 'orden basado en reglas' aumenta las preocupaciones sobre un posible colapso
- El aumento de operaciones encubiertas y actos de sabotaje ponen en riesgo la seguridad de las organizaciones
- Las organizaciones aumentan la preparación para 'escenarios de guerra'
- Ejecutivos y políticos son blanco de actores amenazantes
- La IA llega a su punto de inflexión
- Los empleados con motivaciones ideológicas amenazan cada vez más la seguridad de las organizaciones
- La creciente superposición en las motivaciones de los actores amenazantes
- Uso de drones con fines hostiles
- El uso de redes sociales alimenta el trastorno de la información
- Los eventos de seguridad sanitaria afectan a toda la cadena de suministro

2026

- Los actores amenazantes apuntan a la CNI para maximizar el impacto
- El retroceso en el progreso empresarial en los retos ASG impulsa el activismo
- Los despidos masivos vinculados a la IA aumentan el sentimiento anticorporativo y los riesgos internos
- Aumento de políticas proteccionistas para salvaguardar la resiliencia soberana
- Los actores maliciosos explotan eventos públicos y privados vulnerables
- Las preocupaciones de sostenibilidad interrumpen proyectos de infraestructura intensivos en recursos
- La respuesta de las autoridades ante la amenaza de los drones fomenta una mayor explotación
- Riesgos para las organizaciones derivados de una mayor dependencia de entornos en la nube
- Panorama informativo amenazado por la emergente GenAI
- Las redes sociales se utilizan cada vez más como arma para facilitar campañas masivas de doxxing

Factores de riesgo estratégico

P Político

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- La transición presidencial estadounidense impulsó un cambio hacia el 'transaccionalismo geopolítico', poniendo a prueba las alianzas tradicionales.
- La inestabilidad país/regional (alimentada en gran medida por conflictos) continuó involucrando a potencias internacionales e influyendo en la política y seguridad interna en naciones 'no afectadas'.
- La intensificación de la competencia entre grandes potencias, especialmente China-EE.UU. y Rusia-Occidente, impulsó la recalibración de la política exterior entre regiones y aumentó las actividades de guerra en la zona gris (GZW).

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- El retroceso democrático y los desafíos de gobernanza (incluida la corrupción, la erosión del estado de derecho) aumentarán la probabilidad de disturbios.
- La política radical se vuelve cada vez más común en Occidente, impulsando rápidos cambios regulatorios, disturbios y un discurso polarizado, lo que lleva a la persecución de organizaciones y personas de alto perfil.
- El auge del estilo de liderazgo del 'hombre fuerte', que prioriza la acción unilateral, sigue reforzando la dinámica de 'la fuerza impone la razón', aumentando el riesgo de comportamientos escalatorios, errores de cálculo y conflictos.

E Económico

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- Las medidas comerciales proteccionistas causaron importantes interrupciones en la cadena de suministro, aumentaron costes y redujeron la confianza de los inversores.
- La inflación se alivió en muchas regiones, pero los altos costos de vida y el estancamiento salarial alimentaron el malestar laboral y las huelgas a nivel mundial.
- Los mercados energéticos fluctuantes, impulsados por conflictos, recortes de producción y sanciones, resultaron en costos operativos impredecibles para industrias centradas en energía.

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- La fragmentación continua del comercio global, impulsada por el proteccionismo y la incertidumbre política, probablemente aumentará los costos operativos y dificultará el acceso al mercado.
- La competencia por la capacidad de fabricación de minerales y tecnología crítica se intensificará, influyendo en alianzas económicas.
- Las restricciones fiscales debidas a la alta deuda pública tienen una posibilidad realista de forzar medidas de austeridad, aumentando el riesgo de disturbios.

S Social

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- La movilización digital liderada por la Generación Z impulsó protestas descentralizadas en todo el Sur Global, centradas en agravios distintos y superpuestos, incluyendo corrupción y alto desempleo juvenil.
- El desplazamiento de empleos impulsado por la IA se convirtió en una preocupación pública de alto perfil, ya que los despidos corporativos se vincularon explícitamente a la implementación de sistemas autónomos y agentes de IA.
- La migración y el control fronterizo siguieron siendo una prioridad de seguridad aguda, con desplazamientos a gran escala por conflictos en curso y desastres naturales provocados por el cambio climático.

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- La brecha generacional global se profundizará, con poblaciones jóvenes exigiendo más equidad social, lo que conducirá a un aumento del activismo físico y digital en todo el Sur Global.
- La cohesión social probablemente se deteriorará aún más a medida que el desorden de la información en línea, las presiones económicas y la desconfianza política alimenten la polarización y las narrativas extremistas.
- La reducción de los presupuestos globales de ayuda probablemente pondrá a prueba los esfuerzos humanitarios, aumentando los riesgos de salud y desplazamiento.

Este análisis político, económico, social, tecnológico, ecológico y legal (PESTEL) describe los factores externos clave que se han identificado como moldeadores del entorno operativo empresarial en 2025, y aquellos que se espera que se observen en 2026. Destaca los factores que influyen en la estrategia organizativa, la exposición al riesgo y la toma de decisiones.

Creando para empresas en todo el mundo en todos los sectores.

El análisis destaca cómo la inestabilidad geopolítica, la volatilidad económica, el cambio social, la dependencia tecnológica, la complejidad regulatoria y los factores de estrés medioambientales interactúan para crear riesgos y oportunidades para las organizaciones.

Al identificar los motores estratégicos actuales y sus impactos esperados, este análisis ofrece una visión estructurada de las tendencias a nivel macro que las organizaciones deben monitorizar, adaptar e incorporar en las estrategias de planificación y resiliencia a largo plazo.

T Tecnológico

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- La vulnerabilidad de la infraestructura de tecnología de la información interconectada quedó expuesta por múltiples cortes generalizados de internet, por ejemplo, Cloudflare y fallos importantes de centros de datos.
- El aumento de ciberataques de alto perfil, con ransomware e intrusiones en la cadena de suministro, provocó grandes interrupciones operativas en todos los sectores.
- La competencia por minerales críticos, clave para tecnologías avanzadas y semiconductores, persistió, moldeando la política de seguridad nacional.

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- A medida que las naciones afirman cada vez más su soberanía sobre los sistemas de IA, las organizaciones se enfrentarán a un orden digital cada vez más multipolar, incluyendo requisitos de seguridad, regulaciones y cumplimiento divergentes entre diferentes regiones.
- Acelerar el desarrollo de tecnologías cuánticas intensifica la competencia geopolítica, lo que provoca un aumento de los controles de exportación e incrementa los riesgos de seguridad a largo plazo para las organizaciones.
- La relocalización manufacturera incrementa los costes operativos de las empresas pero fortalece la seguridad de la cadena de suministro.

L Legal

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- Las estructuras de gobernanza global enfrentaron un aumento de la resistencia y el incumplimiento, lo que influyó en rupturas y violaciones de las leyes internacionales.
- La expansión de los regímenes internacionales de sanciones contra industrias estratégicas y Estados-nación continuó intensificándose, generando riesgos operativos y para la movilidad internacional de las empresas.El retraso regulatorio de tecnologías de alto riesgo, incluida la IA, permitió la explotación por parte de actores maliciosos y generó incertidumbre en el cumplimiento normativo.

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- La responsabilidad legal por la negligencia cibernética, las brechas de datos y los daños medioambientales seguirá ampliándose, aumentando los riesgos financieros y reputacionales para las organizaciones.
- Las disputas legales sobre reclamaciones territoriales, derechos marítimos y acceso a recursos probablemente aumentarán, afectando las rutas marítimas y la exposición al riesgo multinacional.
- El uso amplio de los poderes de emergencia por parte del Estado, a menudo introducidos durante periodos de disturbios, probablemente complicará las operaciones empresariales y erosionará las libertades civiles.

E Ecológico

FACTORES ESTRATÉGICOS IDENTIFICADOS EN 2025

- La presión sobre los recursos hídricos alcanzó niveles severos en varias zonas económicas clave (por ejemplo, el sur de Europa, el sur de Asia), lo que provocó cierres localizados de agricultura e industria.
- Casos legales de alto perfil que examinan organizaciones que alegaban reclamaciones de greenwashing sentaron un precedente, creando riesgos reputacionales para la marca.
- La continuación de temperaturas globales extremadamente altas, olas de calor y fenómenos meteorológicos extremos causó graves daños en la infraestructura y problemas en la cadena de suministro.

MOTORES ESTRATÉGICOS ESPERADOS PARA 2026

- Las organizaciones percibidas como cómplices en la causa de la degradación climática se enfrentarán a amenazas crecientes de acciones legales y protestas.
- Los fenómenos meteorológicos extremos y los desastres naturales aumentan en frecuencia e intensidad, alterando las redes logísticas globales, dañando la infraestructura energética y amenazando la seguridad de la fuerza laboral.
- La escasez de recursos provocada por el clima agravará las tensiones transfronterizas y aumentará los riesgos de conflicto.

Seguridad corporativa

1

Los actores amenazantes apuntan a la CNI para maximizar el impacto

Los ataques dirigidos a Infraestructuras Críticas Nacionales (CNI) han aumentado de forma constante a lo largo de 2025, con actores amenazantes explotando tanto tácticas, técnicas y procedimientos (TTPs) cinéticos como no cinéticos. A medida que las tensiones globales por múltiples puntos conflictivos han aumentado, actores amenazantes patrocinados por Estados que operan en la zona gris (GZW), grupos activistas, organizaciones extremistas y actores solitarios han seguido atacando a CNI tradicionales, como energía, agua y comunicaciones, así como a objetivos no tradicionales, como centros de datos y aeropuertos. El acceso facilitado a herramientas de amenazas cibernéticas, así como la prevalencia de sistemas aéreos no tripulados (UAS) comercialmente disponibles, han permitido a los actores amenazantes maximizar el impacto en el CNI con un gasto mínimo.

- Casi con toda seguridad, los actores amenazantes seguirán atacando a CNI, utilizando tanto TTPs tradicionales, como el sabotaje físico, como TTPs no cinéticos, entre ellos malware y ciberataques.
- Es probable que los Estados-nación aumenten el uso de actores actores intermediarios (proxies), como grupos de crimen organizado (GDO), para llevar a cabo sabotaje y ataques disruptivos dirigidos a CNI, con el fin de maximizar la presión política, desestabilizar naciones enemigas y propagar incertidumbre, manteniendo al mismo tiempo una negación plausible.
- Las organizaciones activistas radicales probablemente aumentarán las campañas de sabotaje físico y ciberataques dirigidos a CNI operadas o apoyadas por organizaciones que consideran que actúan en contra de los objetivos de estos grupos, con la intención de causar una disrupción generalizada.

Escenario	Condición del escenario	Probabilidad evaluada
La mejora del panorama geopolítico y sociopolítico impulsa una disminución de los ataques contra CNI, principalmente debido a la reducción del interés y la intención de los activistas. A medida que disminuyen las tensiones, los Estados reducen el uso de actores intermediarios para llevar a cabo acciones de guerra híbrida.	Mejora	Altamente improbable (10%)
Las tensiones globales siguen aumentando, centradas en conflictos y puntos conflictivos en curso, incluyendo cuestiones ambientales, sociales y de gobernanza (ASG); cada vez más activistas tienen como objetivo a la CNI para aumentar la visibilidad de sus causas.	Línea base	Posible / Probable (55%)
Las tensiones geopolíticas se intensifican aún más, lo que lleva a un mayor número de Estados a involucrarse en ataques cada vez más directos contra CNI, incluyendo el despliegue de activos intermediarios como parte de metodologías de ataque más amplias.	Empeora	Improbable (35%)

Recomendación

- Evaluar la exposición de la organización (tanto directa como indirectamente, por ejemplo, a través de socios de la cadena de suministro) a los impactos operativos derivados de interrupciones en las CNI.
- Asegurar que existan mecanismos de contingencia y medidas de mitigación para los flujos de suministro clave (como energía, agua, telecomunicaciones, entre otros), que permitan mantener procesos y capacidades operativas resilientes en caso de afectaciones a la disponibilidad de la CNI.
- Monitorear y mantener conciencia situacional sobre regiones propensas a inestabilidad o disrupciones geopolíticas, especialmente cuando dichas regiones estén vinculadas a la estabilidad operativa. Asimismo, dar seguimiento a los avisos y alertas emitidos por las autoridades gubernamentales en esas zonas.

Indicadores	Implicaciones
— Aumento de la retórica en torno al comercio global, específicamente en relación con aranceles, sanciones y acceso a minerales raros. — Aumento de las tensiones en zonas fronterizas de regiones políticamente volátiles. — Uso más frecuente y generalizado de UAS por parte de actores amenazantes en espacio aéreo restringido. — Aumento de la cobertura en redes sociales que destaca los exitosos ataques del CNI por parte de grupos activistas. — Aumento de la comunicación digital por parte de grupos activistas que asesoran sobre metodologías de ataque dirigidas a CNI y señalan posibles objetivos.	— Las organizaciones responsables o con vínculos con CNI enfrentan un mayor riesgo de ser objetivo de actores amenazantes. — Reducción del acceso a materiales críticos debido al aumento del aislamiento derivado de la actividad hostil de GZW con negación plausible dirigida a CNI. — Interrupción de las capacidades operativas diarias desde impactos hasta comunicaciones CNI. — Aumento del requisito de gastos y responsabilidad legal relacionada con la gestión y operación de los contratos de instalaciones de CNI. — Pérdida de datos e información sensible, y mayor dependencia de factores externos para mantener la integridad de los datos relacionados con el CNI de centros de datos.

El retroceso en el progreso empresarial en los retos ASG impulsa el activismo

Los grupos activistas continúan dirigiendo ataques persistentes contra empresas que se perciben como incumplidoras de sus compromisos Ambientales, Sociales y de Gobernanza (ASG), mediante boicots prolongados, manifestaciones y críticas en línea. A lo largo de 2025, las organizaciones han sido acusadas de retrasar objetivos de cero emisiones netas o de modificar políticas de diversidad, equidad e inclusión (DEI) en respuesta a presiones políticas y económicas, y es casi seguro que estas acusaciones persistirán —y probablemente se intensificarán— durante 2026. Los grupos activistas seguirán señalando a las empresas con medidas cada vez más innovadoras y disruptivas para alcanzar sus objetivos, con un enfoque particular en organizaciones —y personas— que se perciba que están dando marcha atrás en compromisos ASG asumidos previamente.

— Es probable que grupos ambientales, pacifistas o de justicia social inicien o refuercen campañas de boicot, desinversión y sanciones (BDS) dirigidas a organizaciones percibidas como adoptando posturas de menor visibilidad en materia de ASG.

— Las organizaciones que son objeto de estas acciones enfrentan el riesgo de operar en un entorno laboral polarizado, lo que crea condiciones que pueden motivar a actores internos de amenaza a organizar campañas, filtrar comunicaciones internas y participar en actividades de denuncia.

— Es poco probable que las organizaciones puedan reducir silenciosamente sus compromisos ASG sin generar un mayor escrutinio por parte de los grupos activistas. Las presiones externas de accionistas, legisladores e inversionistas probablemente empujarán a las organizaciones a despriorizar o abandonar iniciativas ASG previas, lo que aumentaría el riesgo de ser nuevamente blanco de ataques.

Escenario	Condición del escenario	Probabilidad evaluada
Reducción de la presión activista sobre empresas que retrasan o reducen compromisos ASG a medida que los grupos activistas priorizan otras causas.	Mejora	Altamente improbable (10%)
Las organizaciones que están despriorizando compromisos ASG siguen siendo objetivo de activistas quienes utilizan datos de fuentes abiertas para investigar empresas, utilizando redes sociales para organizar campañas y protestas BDS.	Línea base	Posible / Probable (60%)
Los grupos activistas no ven suficientes avances con los enfoques actuales, y en consecuencia, escalan a tácticas más disruptivas, como el vandalismo, la ocupación de edificios o amenazar la seguridad física de los ejecutivos de la empresa para ejercer presión.	Empeora	Improbable (30%)

Recomendación

— Considerar los riesgos de hacer declaraciones públicas u oficiales sobre temas divisivos o controversiales. Estos pueden atraer la atención de actores amenazantes más comprometidos, que pueden ser más propensos a participar en acciones hostiles o disruptivas.

— Monitorear y evaluar el sentimiento de la fuerza laboral tras anuncios y comunicaciones sobre ASG o temas igualmente emotivos o divisivos, para identificar indicios tempranos de insatisfacción o posibles vectores de amenaza interna.

— Identificar y monitorizar a los actores que puedan ser incitados, influenciados o inspirados a involucrarse en actos hostiles (directa o indirectamente) basándose en políticas e iniciativas organizacionales planificadas.

Indicadores

- Los responsables de políticas a nivel nacional ejercen mayor presión sobre las organizaciones para que reduzcan o abandonen iniciativas ASG.
- Los movimientos activistas amplían su enfoque para incluir entidades secundarias o terciarias asociadas con organizaciones acusadas de despriorizar iniciativas ASG (como socios de la cadena de suministro, aseguradoras, etc.).
- Aumento del enfoque activista sobre individuos (CEOs, miembros del equipo ejecutivo) en lugar de centrarse únicamente en la organización en su conjunto.
- Grupos activistas establecidos anuncian nuevas campañas (o expansiones de campañas existentes) centradas en los retrocesos en iniciativas ASG.

Implicaciones

- Las organizaciones deberán equilibrar las presiones externas de los stakeholders y responsables de políticas con las presiones externas (e internas) de los grupos activistas al comunicar cambios en sus políticas.
- Aumento de los costos de seguridad física para ejecutivos y en las instalaciones (incluidos eventos como juntas de accionistas) durante periodos de crítica significativa.
- Los socios organizacionales (como fundaciones, ONG, etc.) pueden percibir negativamente los retrocesos en ASG, lo que podría generar críticas públicas o la terminación de asociaciones.
- El enfoque persistente de los activistas o el discurso negativo en torno a las organizaciones puede afectar la confianza de consumidores y del mercado, reduciendo los ingresos del negocio.

Los despidos masivos vinculados a la IA aumentan el sentimiento anticorporativo y los riesgos internos

Se espera que la reestructuración impulsada por IA y los despidos masivos continúen durante todo 2026, mientras las organizaciones profundizan su transición hacia la automatización, el despliegue de IA generativa y la expansión de centros de datos, corrigiendo al mismo tiempo la sobrecontratación durante la pandemia. Es probable que estas reducciones intensifiquen el sentimiento anticorporativo, aumenten los riesgos internos y generen agitación entre los grupos activistas anti-IA redes de derechos laborales.

Estas condiciones crean una mayor vulnerabilidad durante periodos de interrupción en la fuerza laboral, mientras que las redes activistas organizan cada vez más la oposición a la rápida adopción de la IA.

- La reducción de la fuerza laboral impulsada por IA, principalmente en tecnología, manufactura, atención al cliente y logística, está aumentando los riesgos internos como el robo de datos, el sabotaje y el mal uso de herramientas de IA. La creciente sofisticación de estas tácticas supone una amenaza creciente para la estabilidad financiera, legal y reputacional, mientras que en los grupos anti-IA y de derechos laborales es posible que intensifiquen la presión a través de campañas y huelgas en línea.
- Los incidentes internos localizados son una posibilidad realista, mientras que los disturbios a gran escala siguen siendo poco probables; sin embargo, pueden producirse impactos operativos significativos en centros de datos, servicios digitales y entornos de producción automatizados relacionados con el sentimiento anti-IA (incluidas acciones no internas).
- El sabotaje interno en entornos habilitados por IA tiene el potencial de provocar interrupciones a nivel organizacional y sectorial, mientras que la creciente complejidad de las estrategias y tácticas activistas, junto con el aumento de factores de riesgo interno, representa una amenaza creciente para la estabilidad operativa en industrias que atraviesan una transformación rápida impulsada por la IA.

Escenario	Condición del escenario	Probabilidad evaluada
Los despidos impulsados por la IA disminuyen a medida que la planificación de la fuerza laboral se estabilice, reduciendo la exposición a riesgos internos y disminuyendo el sentimiento anticorporativo.	Mejora	Altamente improbable (10%)
La reestructuración relacionada con la IA continúa a un ritmo constante-moderado, manteniendo un riesgo interno moderado, críticas continuas en línea y presión activista periódica.	Línea base	Posible / Probable (50%)
Despidos visibles o repetidos aumentan el sentimiento anticorporativo, provocando un aumento de incidentes internos y campañas activistas más coordinadas dirigidas a activos y reputaciones corporativas.	Empeora	Improbable (40%)

Recomendación

- Mantener una postura de seguridad reforzada mediante el fortalecimiento de la supervisión de amenazas internas, el endurecimiento de los controles de acceso y el aumento de la visibilidad sobre los sistemas habilitados con IA, con el fin de reducir las oportunidades de uso indebido o sabotaje durante disrupciones en la fuerza laboral.
- Mantener un relacionamiento regular con autoridades y entes reguladores para recibir lineamientos actualizados y coordinar medidas preventivas, asegurando que las instalaciones, centros de datos y entornos automatizados estén protegidos frente a amenazas emergentes.
- Reforzar la resiliencia operativa y de la cadena de suministro mediante la identificación de dependencias críticas, la revisión de planes de contingencia y la preparación de alternativas que mitiguen interrupciones derivadas de acciones internas o interferencias de grupos activistas.

Indicadores	Implicaciones
— Aumentar la reducción de la fuerza laboral vinculada a la IA en los sectores tecnológico, manufacturero y de servicios en regiones con automatización avanzada. — Más organizaciones que defienden y promueven públicamente su uso de herramientas de IA en roles que antes desempeñaban empleados humanos. — Comentarios públicos, políticos y de activistas crecientes que critican la rápida adopción de la IA, con grupos laborales organizados y que coordinan campañas en contra de estrategias de automatización corporativas. — Aumento de incidentes de riesgo interno, incluyendo robo de datos, uso indebido de accesos o sabotaje vinculado a empleados desplazados o insatisfechos.	— Aumento de los requisitos y presupuestos de seguridad, especialmente para la monitorización de amenazas internas, controles de acceso y protección de infraestructuras habilitadas por IA. — Mayor probabilidad de interrupciones operativas, incluyendo caídas en centros de datos, fallos en la cadena de suministro debido a sabotaje interno o acciones de activistas externos, o interferencias en entornos de producción automatizados. — Riesgos regulatorios y reputacionales elevados, lo que lleva a las empresas a reforzar la planificación del impacto en los empleados y la comunicación pública en torno a la adopción de la IA.

Aumento de políticas proteccionistas para salvaguardar la resiliencia soberana

El aumento de las políticas proteccionistas, impulsado por la intensificación de las tensiones geopolíticas, consideraciones de seguridad nacional y objetivos de soberanía, ha incrementado la volatilidad de los mercados y ha introducido un mayor nivel de incertidumbre económica para las organizaciones a lo largo de 2025. Se prevé que esta tendencia continúe durante 2026, reflejando el uso creciente del comercio por parte de los gobiernos como herramienta de presión política, así como la relocalización y nacionalización de la manufactura y los servicios para fortalecer la seguridad nacional y la resiliencia soberana.

- Es probable que los líderes globales continúen implementando políticas proteccionistas a medida que persistan las tensiones geopolíticas y sociopolíticas. Este enfoque previsiblemente seguirá agravando problemáticas existentes, como las vulnerabilidades en las cadenas de suministro, el uso de acuerdos comerciales como mecanismo de negociación y la imposición de embargos o aranceles sobre recursos estratégicos.
- Los impactos de largo plazo de la adopción generalizada de políticas proteccionistas tienen el potencial de impulsar cambios en la estrategia corporativa, a medida que el comercio transfronterizo se vuelve más complejo o costoso. Esto puede llevar a que las organizaciones exploren soluciones “in-country” (dentro del país), lo que podría deteriorar aún más las relaciones comerciales globales y exponer las cadenas de suministro en proceso de adaptación a actores de amenaza.
- La relocalización (reshoring) de industrias esenciales para la preservación de las capacidades de defensa y el mantenimiento de CNI probablemente seguirá siendo un eje central de futuras políticas proteccionistas. No obstante, esto podría incrementar los costos y exponer a las organizaciones a complejidades derivadas de cambios rápidos en la oferta y la demanda.

Escenario	Condición del escenario	Probabilidad evaluada
Las tensiones geopolíticas y sociopolíticas disminuyen, reduciendo la volatilidad del mercado. El comercio transfronterizo se estabiliza, con una tendencia a la baja en el uso de aranceles y embargos.	Mejora	Altamente improbable (15%)
Los líderes políticos continúan imponiendo políticas proteccionistas esporádicas, obligando a las organizaciones a adaptar continuamente sus operaciones y reevaluar las relaciones comerciales, lo que genera incertidumbre.	Línea base	Posible / Probable (55%)
El comercio se utiliza cada vez más como palanca política, creando una incertidumbre ingobernable en los mercados globales. Las cadenas de suministro se ven significativamente alteradas debido a las condiciones comerciales que cambian rápidamente.	Empeora	Improbable (30%)

Recomendaciones

- Garantizar que todas las operaciones sean receptivas y adaptables a cambios regulatorios y establecer planes de contingencia realistas en caso de que las políticas proteccionistas afecten la capacidad operativa.
- Implementar procedimientos de seguridad robustos en torno a las cadenas de suministro y los almacenes para evitar que los actores peligrosos exploten vulnerabilidades durante los periodos de transición posteriores al anuncio de dichas políticas.
- Coordinarse con socios internacionales para establecer planes de respuesta a incidentes (IRP) que permitan la continuidad operativa a pesar de la incertidumbre.

Indicadores	Implicaciones
— Incremento regional del populismo nacionalista que promueve la desglobalización de las industrias. — Cancelación más frecuente de contratos alegando preocupaciones de seguridad. — Comportamientos controvertidos por parte de territorios u organizaciones con los que otros países no desean ser considerados cómplices. — Puntos críticos globales que requieren negociaciones políticas. — Aumento de políticas proteccionistas por parte de aliados económicos, lo que incentiva la adopción de medidas de represalia. — Creciente preocupación por el acceso a datos y el espionaje asociado a bienes importados.	— Deterioro de la cooperación transfronteriza, lo que frena la innovación y el desarrollo en las industrias objetivo. — Incremento del valor estratégico de las importaciones y exportaciones, explotado por actores de amenaza que convergen dimensiones cibernéticas y físicas para mantenerse indetectados. — Incertidumbre sostenida en torno a la rentabilidad, la relación oferta-demanda y los estándares regulatorios. — Disminución significativa de la inversión extranjera directa (IED). — Consecuencias financieras y operativas de mayor alcance para filiales, inversionistas y proveedores terceros, a medida que las expectativas corporativas se ajustan a los marcos de política pública.

Los actores maliciosos explotan eventos públicos y privados vulnerables

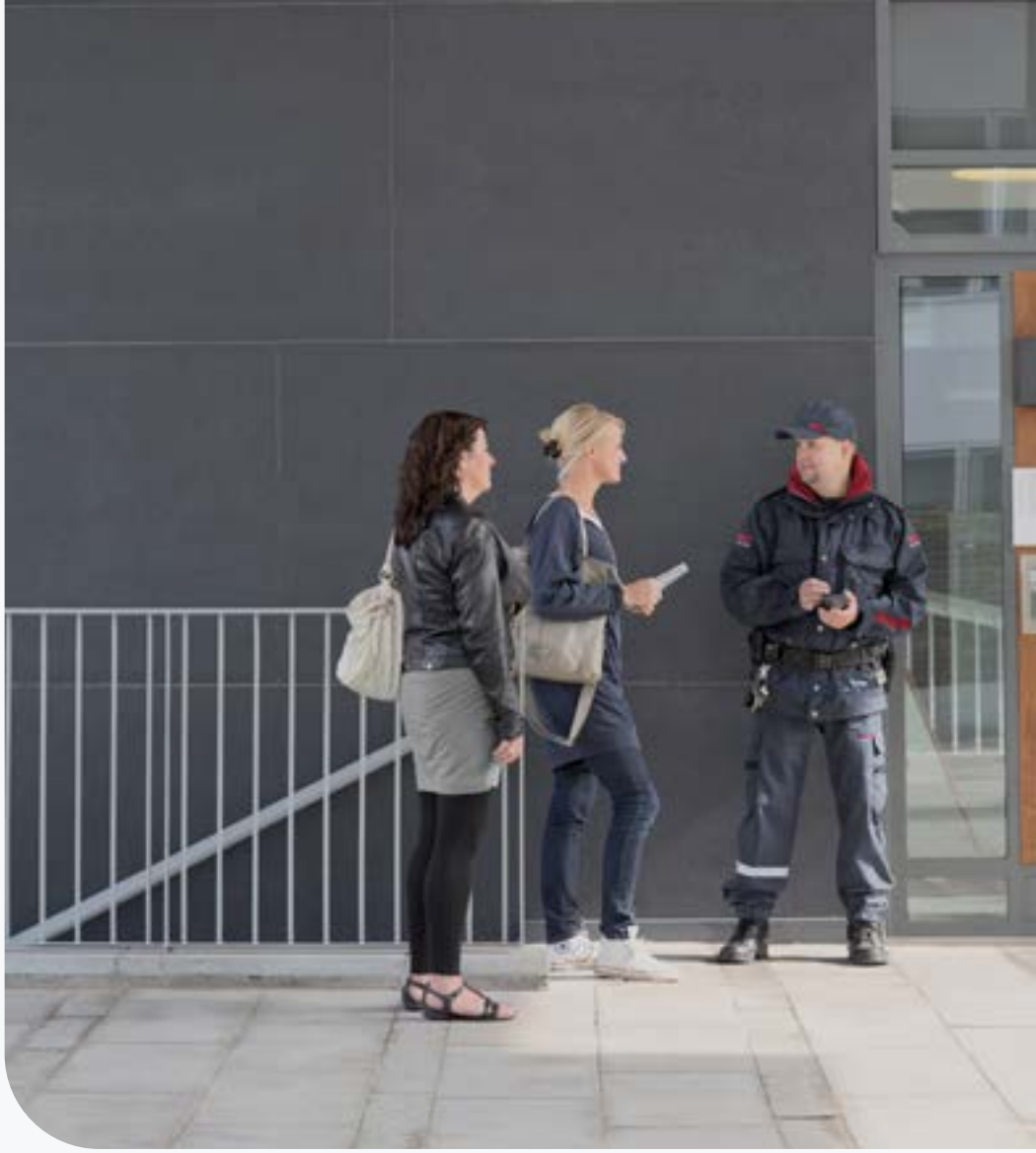
En los últimos años, los actores malintencionados han atacado cada vez más eventos a gran escala debido a su accesibilidad, la posibilidad de que haya objetivos de alto valor presentes y la oportunidad de dar a conocer sus acciones para ganar impacto en redes sociales. Las tensiones geopolíticas en curso y los problemas sociopolíticos divisivos, como la protección del medio ambiente y el desarrollo de la inteligencia artificial (IA), seguirán siendo motores clave del activismo y las amenazas internas durante 2026. Además de las tácticas, técnicas y procedimientos (TTPs) existentes, los actores amenazantes casi con toda seguridad seguirán evolucionando su enfoque mediante métodos innovadores, cómo aprovechar el aumento de preocupaciones como oportunidad para emitir amenazas falsas y causar interrupciones.

- Si bien la focalización de eventos en función de la asistencia corporativa ha sido utilizada por grupos activistas durante muchos años, otros perfiles de actores de amenaza son cada vez más propensos a adoptar esta táctica como un medio para acceder a individuos clave o activos estratégicos en entornos menos controlados.
- La participación de grandes organizaciones en eventos incrementa el riesgo de espionaje corporativo sobre información sensible, la cual podría ser utilizada posteriormente para causar daños reputacionales, ejercer extorsión o ser comercializada con empresas competidoras.
- Es probable que los actores amenazantes cada vez más ingeniosos utilicen múltiples fuentes de datos para recopilar información sobre su objetivo, como identificar hoteles cercanos a un evento donde un objetivo probablemente se aloje, o rutas de transporte probables hacia y desde el evento. Esto puede usarse para realizar acciones vinculadas a, pero alejadas del propio evento.

Escenario	Condición del escenario	Probabilidad evaluada
La mejora de la postura de seguridad para los eventos y los objetivos de alto valor impulsa a los actores amenazantes a buscar otras vías de ataque debido a las menores tasas de éxito percibidas.	Mejora	Altamente improbable (10%)
Los actores amenazantes continúan atacando e interrumpiendo eventos, empleando TTPs nuevos y existentes. Los eventos siguen sufriendo interrupciones tanto por la intervención de los actores amenazantes como por el reforzamiento de los protocolos de seguridad.	Línea base	Posible / Probable (60%)
Los actores de amenaza logran éxitos reiterados al focalizar eventos. La percepción de una mayor efectividad impulsa nuevos intentos, incrementando los niveles de disrupción. Como consecuencia, incluso eventos que no son objetivo directo pueden verse significativamente afectados debido al refuerzo de las medidas de seguridad implementadas en respuesta al aumento del nivel de amenaza.	Empeora	Improbable (30%)

Recomendaciones

- Mejorar la seguridad operativa (OPSEC) en torno a la asistencia a eventos externos, reduciendo la divulgación de detalles específicos del evento (como los asistentes). Evitar compartir públicamente detalles como pases o acreditaciones para eventos en redes sociales.
- Considerar verificaciones de antecedentes adecuadas de los asistentes para reducir la posibilidad de que los actores malintencionados tengan acceso legítimo a un evento.
- Garantizar que las medidas de seguridad para los objetivos de alto valor no comiencen ni terminen ‘en la puerta’, considerando la posibilidad de que actores de amenaza realicen acciones de focalización fuera del evento, en sus inmediaciones o durante los desplazamientos de ida y regreso.



Indicadores

- Incremento en la focalización de cuentas vinculadas a eventos en redes sociales, en función de las personas u organizaciones asistentes.
- Aumento de reportes sobre eventos a los que asisten o que son objetivo de actores de amenaza no activistas, como clientes inconformes, elementos criminales y personas con conductas obsesivas.
- Escalada en las tácticas, técnicas y procedimientos (TTP) utilizados por actores de amenaza que buscan interrumpir eventos.
- Aparición de puntos críticos en los factores detonantes (como conflictos geopolíticos) en la antesala o durante el desarrollo de los eventos.
- Movimientos de boicot dirigidos contra organizaciones secundarias o terciarias, así como contra los organizadores del evento y los hoteles que alojan a los asistentes.

Implicaciones

- Requisitos de seguridad reforzados para quienes organizan o asisten a eventos, lo que resulta en un aumento de los presupuestos de seguridad.
- Procesos más estrictos de solicitud y evaluación de los asistentes afectan la accesibilidad al público y a organizaciones externas, lo que podría generar críticas.
- Las organizaciones consideran cada vez más cambiar los eventos a plataformas online para minimizar la posibilidad de interrupciones.
- Las organizaciones se vuelven reacias a enviar ejecutivos de alto perfil a eventos públicos debido a preocupaciones de seguridad.

Las preocupaciones en materia de sostenibilidad interrumpen proyectos de infraestructura intensivos en recursos

La demanda de proyectos de infraestructura que requieren un uso intensivo de recursos —como centros de datos, generadores de energía renovable y plantas de semiconductores— aumentará a lo largo de 2026. Esto se deberá a que los gobiernos subvencionarán proyectos por razones estratégicas y económicas, y a que las organizaciones continuarán su transición hacia servicios y operaciones impulsados por la IA.

Estos proyectos exigen recursos sustanciales, incluyendo energía, agua, suelo y minerales críticos, lo que incrementa las preocupaciones sobre sostenibilidad por parte de reguladores, líderes políticos y actores socioeconómicos, incluidos los activistas ambientales y la fuerza laboral.

— Este crecimiento está impulsado por la "carrera armamentista" digital y de IA a nivel geopolítico estratégico, y a nivel de mercado por organizaciones que impulsan sus estrategias digitales y de IA para ganar competitividad —lo que aumenta la demanda de centros de datos y semiconductores—. Asimismo, influyen las transiciones en curso hacia tecnologías de energía limpia, como los vehículos eléctricos y la generación de energía renovable, que requieren minerales críticos.

— La intensidad de recursos de estos proyectos de infraestructura ha provocado protestas, sabotajes, demandas e investigaciones por parte de activistas, reguladores y gobiernos debido a su impacto en el suministro de agua, los recursos energéticos, la disponibilidad de suelo y los residuos. Además, representan objetivos de alto valor (HVT, por sus siglas en inglés) para actores estatales y tácticas de espionaje y sabotaje; lo cual, aunque no esté motivado por preocupaciones de sostenibilidad, resalta la criticidad del sector.

— La expansión continua de estos proyectos en 2026 generará una presión creciente sobre los desarrolladores y los gobiernos para implementar restricciones ambientales más estrictas. Esto pone en riesgo de retraso los planes de transición digital y de IA, y endurece los procesos de aprobación para proyectos futuros, a pesar del percibido retroceso en los compromisos ASG a nivel global.

Escenario	Condición del escenario	Probabilidad evaluada
Los avances tecnológicos o los cambios en la demanda global conducen a una reducción de los proyectos de infraestructuras intensivos en recursos, disminuyendo las preocupaciones sobre la sostenibilidad.	Mejora	Altamente improbable (10%)
Las demandas globales de infraestructuras continúan al ritmo actual, lo que lleva a una mayor expansión de los proyectos de construcción y a un aumento del escrutinio tanto en el discurso político como en el público.	Línea base	Posible / Probable (65%)
El crecimiento de la demanda se acelera significativamente, lo que provoca una mayor presión sobre los recursos, provocando interrupciones empresariales, retórica política polarizada y un activismo intensificado.	Empeora	Improbable (25%)

Recomendaciones

— Evaluar la exposición a infraestructuras con uso intensivo de recursos, particularmente en regiones sujetas a una mayor controversia en torno a la presión sobre los recursos y el daño ambiental.

— Mantener el monitoreo de la percepción en línea (online sentiment) respecto a los proyectos de infraestructura, incrementando la participación a nivel local para abordar las preocupaciones sobre sostenibilidad, incluyendo una comunicación transparente sobre los requisitos de recursos, los cronogramas del proyecto y los beneficios económicos.

— Monitorear posibles cambios en las regulaciones sobre el uso de recursos e impactos ambientales para mitigar afectaciones operativas en los cronogramas de los proyectos y las interrupciones en la cadena de suministro.

Indicadores	Implicaciones
— Aumento en la construcción de nuevos centros de datos, productos dependientes de semiconductores y proyectos de energía renovable. — Mayor escrutinio sobre la escasez de agua, las limitaciones de capacidad de la red eléctrica o las disputas por el uso del suelo en torno a los sitios de los proyectos, tanto en medios de comunicación como en redes sociales. — Incremento de la actividad de protesta, incluidas campañas a nivel local y demandas judiciales dirigidas contra los proyectos y las empresas involucradas. — Aumento de moratorias o bloqueos por parte de jurisdicciones locales a proyectos de infraestructura planificados debido a la oposición local. — Crecimiento de narrativas de teorías conspirativas en torno a la infraestructura y las tecnologías asociadas.	— El escrutinio sostenido conduce a cambios en las políticas y a requisitos de sostenibilidad más estrictos. — Aumento de los costos de los proyectos y retrasos en proyectos de infraestructura, a medida que se endurecen las regulaciones y se prolongan los procesos de aprobación y zonificación. — Las empresas dependientes de esta infraestructura enfrentan cuellos de botella en el suministro y proveedores inestables. — Incremento en la frecuencia, escala e intensidad de la actividad de grupos activistas contra desarrolladores, lo que agrava los retrasos. — Mayor amenaza de actos extremistas, incluidos sabotajes y acciones destructivas.

La respuesta de las autoridades ante la amenaza de los drones fomenta un mayor uso de estos.

La continua reticencia de las autoridades occidentales para enfrentar las amenazas que representan los drones para nodos de transporte, instalaciones militares y otros componentes de CNI, junto con los avances tecnológicos en los sistemas UAS, seguirá proporcionando a actores de amenaza —incluidos activistas, terroristas e individuos patrocinados por Estados— oportunidades para llevar a cabo acciones disruptivas a lo largo de 2026. El aumento de la actividad no autorizada de drones sobre sitios sensibles en los últimos años ha incrementado la preocupación por los impactos más amplios sobre las entidades afectadas, contribuyendo a un mayor nivel de incertidumbre en un contexto de críticas a la capacidad de las autoridades para abordar las amenazas híbridas percibidas.

- La disponibilidad comercial y los avances en las capacidades de los UAS impulsarán una mayor evolución de las tácticas, técnicas y procedimientos (TTP) en el empleo de drones, con actores de amenaza —incluidas organizaciones criminales— que utilizarán equipos desechables lanzados localmente para atacar objetivos residenciales, recreativos, comerciales e industriales.
- Individuos altamente motivados continuarán demostrando su capacidad para utilizar los UAS como una forma alternativa de protesta, explotando la ansiedad pública para maximizar la visibilidad y generar atención mediática, así como para registrar activos, documentar reclamos y otorgar credibilidad a narrativas críticas.
- El impacto de las interrupciones operativas debidas a avistamientos sospechosos de drones alrededor del CNI y nodos de transporte probablemente seguirá siendo explotado y utilizado como arma por actores estatales hostiles que buscan participar en una guerra híbrida o de zona gris (GZW).

Escenario	Condición del escenario	Probabilidad evaluada
Despliegue generalizado de equipos especializados contra drones, así como disposiciones que aseguren a las partes afectadas la autoridad y capacidad para interceptar drones de forma segura. Las autoridades implementan reglas claras de enfrentamiento para actividades sospechosas de UAS.	Mejora	Altamente improbable (10%)
Los adversarios continúan explotando la vacilación, probando capacidades de detección y respuesta a drones y compromisos con los acuerdos colectivos de defensa, definiendo los umbrales para el combate.	Línea base	Posible / Probable (80%)
Escalada causada por una colisión de dron (accidental o deliberada). Falta de implementar disuasiones efectivas conduce a un mayor impacto en el CNI y el transporte hubs de UAS y sistemas de 'interferencia' conducen a un despliegue más generalizado por parte de actores amenazantes.	Empeora	Improbable (10%)

Recomendaciones

- Realizar una revisión de las vulnerabilidades frente al reconocimiento aéreo, asegurando que se implementen procedimientos para gestionar incursiones en el espacio aéreo sobre las instalaciones y que los activos sensibles o confidenciales no queden expuestos a la vista.
- Mantener conocimiento actualizado de la normativa que regula las restricciones del espacio aéreo sobre las propiedades, garantizando que el personal esté capacitado y cuente con los medios necesarios para gestionar situaciones relacionadas con despliegues de sistemas UAS, incluidos casos como los de supuestos "auditores de seguridad".
- Mantener monitoreo sobre contenido en línea que exponga perímetros del sitio o medidas de seguridad internas, el cual podría ser utilizado para actividades ofensivas, labores adicionales de reconocimiento o la planificación de protestas y acciones directas.

Indicadores	Implicaciones
— Mayor uso de drones para reconocimiento hostil para informar acciones dirigidas a los sitios. — Mayor disponibilidad y acceso a la tecnología UAS, especialmente unidades que podrían percibirse como más baratas o 'desechables'. — El aumento de la conciencia situacional y la continua escalada de tensiones contribuyen a un mayor número de reportes de actividad sospechosa de drones atribuida a actores estatales hostiles, lo que incrementa el interés y la demanda por sistemas de detección de UAS. — La persistente controversia en torno a las atribuciones de las autoridades militares para hacer frente a amenazas con drones, especialmente en sitios sensibles ubicados en zonas urbanas adyacentes a poblaciones civiles.	— Riesgo continuo de cierre de espacio aéreo como resultado de actividad sospechosa de drones, con actores no malintencionados que causan inadvertidamente interrupciones en medio de una creciente ansiedad. — Creciente escrutinio sobre los sistemas comerciales de detección de drones, especialmente la tecnología desarrollada por empresas con sede en estados percibidos como hostiles por los gobiernos occidentales. — Mayor interés por la inversión antidrones para proteger activos críticos offshore / rutas de tránsito. — Exposición en línea de medidas de seguridad in situ que podrían ser explotadas por otros actores amenazantes.

Riesgos para las organizaciones derivados de una mayor dependencia de entornos en la nube

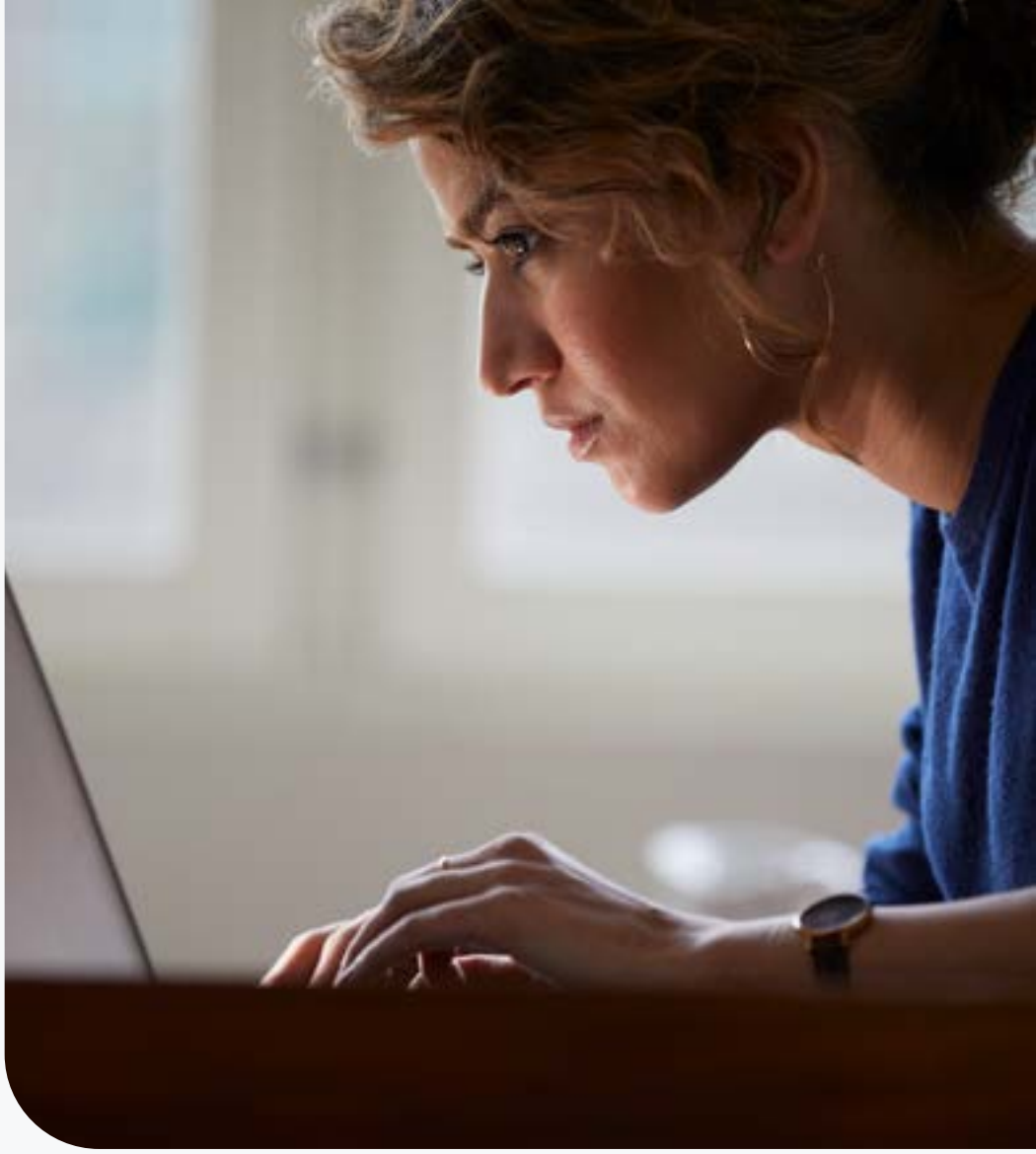
Las amenazas cibernéticas para las empresas aumentarán a medida que más organizaciones migren sus operaciones a modelos de Software como Servicio (SaaS) basados en la nube, incrementando la exposición a riesgos asociados a los servicios cloud, como interrupciones del servicio, brechas de seguridad y configuraciones incorrectas. La infraestructura digital se encuentra altamente concentrada en grandes proveedores de nube como Amazon Web Services (AWS), Microsoft Azure y Google; sin embargo, muchas compañías utilizan múltiples plataformas, lo que amplía su superficie de exposición a riesgos digitales. Este escenario se ve agravado a medida que las empresas consolidan esquemas de trabajo híbrido e integran Inteligencia Artificial (IA) en sus operaciones.

- La IA generativa aumentará la amenaza de robo de credenciales y phishing, ya que hace que estas tácticas sean más accesibles y efectivas mediante automatización, reduciendo el umbral técnico para que los ataques sean viables.
- La infraestructura digital basada en la nube es propensa para este tipo de ataques, ya que los delincuentes pueden explotar errores humanos actuando rápidamente, dificultando la detección y prevención, y dejando vulnerables grandes cantidades de datos sensibles y sin encriptar.
- La rápida migración de las empresas a múltiples proveedores SaaS seguirá creando considerables puntos ciegos en torno a los privilegios de gestión de Identidad y Acceso (IAM), aumentando las amenazas cibernéticas e internas.
- Las interrupciones en la nube seguirán ocurriendo de forma esporádica, interrumpiendo gravemente las operaciones de la empresa y aumentando la probabilidad de ataques que busquen explotar estas interrupciones.

Escenario	Condición del escenario	Probabilidad evaluada
Las organizaciones reconocen la creciente amenaza e invierten lo suficiente en la seguridad en la nube, reduciendo la amenaza de brechas de datos. Los proveedores mejoran la seguridad y las medidas técnicas de seguridad para mitigar y evitar incidentes.	Mejora	Altamente improbable (15%)
Las empresas continúan migrando a proveedores SaaS basados en la nube, aumentando el impacto global de los incidentes e interrupciones de seguridad, generando brechas de datos y amenazas cibernéticas cada vez más significativas.	Línea base	Posible / Probable (70%)
Los problemas con los proveedores de la nube se vuelven más frecuentes, incluyendo una pérdida de datos a gran escala. Las empresas se ven obligadas a desvincular sus operaciones de los sistemas basados en la nube.	Empeora	Improbable (15%)

Recomendaciones

- Garantizar que todo el personal, así como terceros / proveedores, estén informados y actualizados sobre los procesos y prácticas de protección de datos y ciberseguridad, como la fuerza de las contraseñas y la identificación y verificación de solicitudes de credenciales.
- Formar a los empleados en la detección de tácticas de suplantación impulsadas por IA, como llamadas deepfake, intentos de phishing o vishing.
- Invertir en herramientas modernas y automatizadas de seguridad en la nube, como la gestión de postura de seguridad en la nube (CSPM) y la autenticación multifactor (MFA).
- Garantizar que existan planes de contingencia y medidas de seguridad operativas para minimizar las interrupciones durante las interrupciones en la nube.



Indicadores

- Las organizaciones aceleran el paso hacia múltiples sistemas en la nube SaaS.
- Las interrupciones y brechas en la nube ocurren con mayor frecuencia, provocando interrupciones multisectoriales y facilitando ataques oportunistas adicionales.
- El creciente deseo por parte de las autoridades y gobiernos de legislar hacia medidas de seguridad y técnicas más robustas para garantizar la continuidad de la provisión y protección de datos dentro de los servicios en la nube, incluyendo importantes repercusiones legales y financieras por fallos.
- Un ataque, una interrupción o una brecha de seguridad importante genera incertidumbre en la industria respecto a la sobremigración hacia los servicios en la nube.

Implicaciones

- Las interrupciones de la nube provocan una gran interrupción en las operaciones empresariales en múltiples sectores, incluyendo el gobierno e infraestructuras nacionales críticas.
- Las empresas se enfrentan a amenazas persistentes derivadas de brechas y fugas de datos posteriores, lo que podría exponerlas a costes legales significativos, daños reputacionales y probable pérdida de negocio.
- Las organizaciones se enfrentan a riesgos financieros reputacionales por no cumplir con los requisitos regulatorios como las leyes de protección de datos.
- Las empresas deben reajustar su gasto en seguridad para mitigar el aumento de la amenaza cibernética y las consecuencias asociadas.

Panorama informativo amenazado por la emergente IA generativa (GenAI)

Las capacidades de la Inteligencia Artificial (IA) avanzan más rápido que la capacidad de la sociedad para distinguir contenido auténtico de contenido fabricado por IA. Es probable que esta aceleración tecnológica choque con una disminución sostenida de la confianza institucional, creando condiciones en las que las empresas se enfrenten a amenazas tangibles y disruptivas como ataques a la reputación, manipulación del mercado y disrupciones operativas. El panorama informativo seguirá fracturándose, ya que los medios tradicionales ven deteriorados en su credibilidad y la creciente influencia dominante de fuentes alternativas no verificadas persiste y probablemente aumente aún más.

— La confianza y el compromiso con las instituciones mediáticas tradicionales ha alcanzado mínimos históricos. Este vacío se está llenando cada vez más gracias a influencers, periodistas civiles que operan sin supervisión editorial y medios alternativos, muchos de los cuales dominan audiencias mayores que los grandes periódicos y priorizan la participación sobre la verificación.

— Los actores estatales y no estatales poseen capacidades sofisticadas de IA generativa y han demostrado la intención de manipular entornos de información. Ecosistemas mediáticos alternativos en plataformas como Telegram, X y redes descentralizadas emergentes probablemente servirán como canales principales de distribución.

— Las herramientas de clonación de voz, intercambio de rostros y generación de texto permiten a cualquier actor motivado crear contenido sintético convincente de ejecutivos, funcionarios o figuras públicas en cuestión de horas. Las empresas en 2026 y más allá probablemente se enfrentarán a ataques regulares de medios sintéticos, incluidos aquellos destinados a interrumpir operaciones o extraer información sensible.

Escenario	Condición del escenario	Probabilidad evaluada
La tecnología de detección sigue el ritmo de las capacidades de la IA, limitando el impacto del contenido sintético, y las políticas de las plataformas crean barreras efectivas, ya que el público desarrolla hábitos de verificación a través de la alfabetización mediática.	Mejora	Altamente improbable (20%)
Los ataques a medios sintéticos aumentan significativamente pero siguen siendo manejables, ya que la detección lucha por igualar la calidad de generación, aunque ofrece cierta protección. Sin embargo, los incidentes corporativos de alto perfil siguen causando interrupciones.	Línea base	Posible / Probable (40%)
El contenido sintético supera los sistemas de detección y verificación y la confianza pública se erosiona aún más. Los ataques a organizaciones facilitados por contenido generado aumentan en tanto la frecuencia como la eficacia.	Empeora	Improbable (40%)

Recomendaciones

— Implementar autenticación multinivel para las comunicaciones ejecutivas, incluyendo canales verificados que las partes interesadas sepan consultar durante las crisis. Establecer sistemas de palabras clave para comunicaciones sensibles que no puedan replicarse en deepfakes.

— Desarrollar herramientas para monitorizar plataformas sociales y de medios alternativos para menciones de marcas y ejecutivos e identificar procesos para identificar/informar/eliminar contenido generado.

— Limitar la exposición ejecutiva en entornos no controlados que probablemente proporcionen material fuente de alta calidad para deepfakes. Revisa las apariciones públicas y los compromisos para grabar los controles.

Indicadores	Implicaciones
— Aumento de la prevalencia y el acceso a herramientas para la creación de contenidos generativos. — Las audiencias de los creadores de medios alternativos superan a las de los medios tradicionales, y los algoritmos de las plataformas priorizan el contenido de periodistas civiles e influencers sobre los medios tradicionales. — Las crisis corporativas se originan cada vez más en fuentes alternativas en lugar de la información tradicional. Los estándares de verificación disminuyen y los medios sintéticos circulan ampliamente antes de ser desacreditados. — Los grupos de actores amenazantes utilizan cada vez más capacidades GenAI para difundir desorden informativo, permitir acciones hostiles y atacar reputaciones corporativas.	— La confianza y la moral de los empleados se ven afectadas a la comunicación interna del contenido sintético. El personal descontento amplifica o incluso genera medios sintéticos para atacar a su propia organización. — Las amenazas internas aumentan ya que los empleados no pueden verificar las comunicaciones con los directivos. — Las teorías conspirativas y los deepfakes socavan la confianza pública y económica. — Las campañas de medios sintéticos se dirigen a socios de la cadena de suministro con afirmaciones falsas sobre calidad, seguridad o prácticas empresariales. Las relaciones B2B se ven afectadas si la autenticación de las comunicaciones con socios se vuelve poco fiable.

Las redes sociales se utilizan cada vez más como arma para facilitar campañas masivas de doxxing

El uso de las redes sociales para facilitar campañas de misinformación, desinformación y malinformación se incrementó de forma significativa en 2025, a medida que las mejoras en la tecnología de IA generativa han permitido crear, amplificar e instrumentalizar narrativas con mayor velocidad y alcance. Esta rápida amplificación también puede impulsar campañas de doxxing dirigidas, en las que contenido falso o incendiario se utiliza para justificar la exposición de información personal identificable (PII) de un individuo en redes sociales y movilizar acciones de acoso.

- Las herramientas de IA (incluyendo grandes modelos de lenguaje de acceso gratuito como ChatGPT, Gemini y Grok) pueden utilizarse para buscar información personal e identificable de personas o empresas de interés, y si no se implementan (o se eluden barreras de privacidad), pueden encontrar datos precisos como números de contacto, apellidos familiares y direcciones residenciales
- Las secuelas del asesinato de Charlie Kirk ponen de manifiesto el uso creciente de las redes sociales para identificar objetivos de acciones de represalia como el acoso coordinado, el doxxing y la intimidación en el mundo real por parte de actores que buscan explotar el aumento del sentimiento público.
- La persistente polarización sociopolítica, junto con el aumento de la inseguridad económica — real o percibida—, probablemente alimentará un mayor descontento y una intensificación del sentimiento negativo hacia determinadas organizaciones. Esto muy probablemente derivará en un aumento de la focalización de CEOs y altos ejecutivos como la "cara pública" de las compañías.
- Las diferentes leyes de privacidad y protección de datos harán que la aplicación y regulación constantes sean un desafío, lo que podría llevar a los gobiernos a considerar restricciones o limitaciones en las plataformas de redes sociales.

Escenario	Condición del escenario	Probabilidad evaluada
Las leyes más estrictas de protección de datos reducen el acceso público a la información personal identificable (PII), y la legislación refuerza la transparencia de las plataformas en materia de moderación y algoritmos, incorporando normas y sanciones más severas contra el acoso, hostigamiento en línea y el doxxing.	Mejora	Altamente improbable (20%)
Los actores de amenaza continúan explotando las redes sociales para facilitar la rápida difusión de información personal identificable (PII) de ejecutivos corporativos y oponentes políticos, lo que incrementa los riesgos para la seguridad física de las personas afectadas y genera disrupciones para las organizaciones.	Línea base	Posible / Probable (55%)
Los actores de amenaza utilizan cada vez más las redes sociales para llevar a cabo campañas de doxxing motivadas por injusticias organizacionales percibidas y disputas sociopolíticas.	Empeora	Improbable (25%)

Recomendaciones

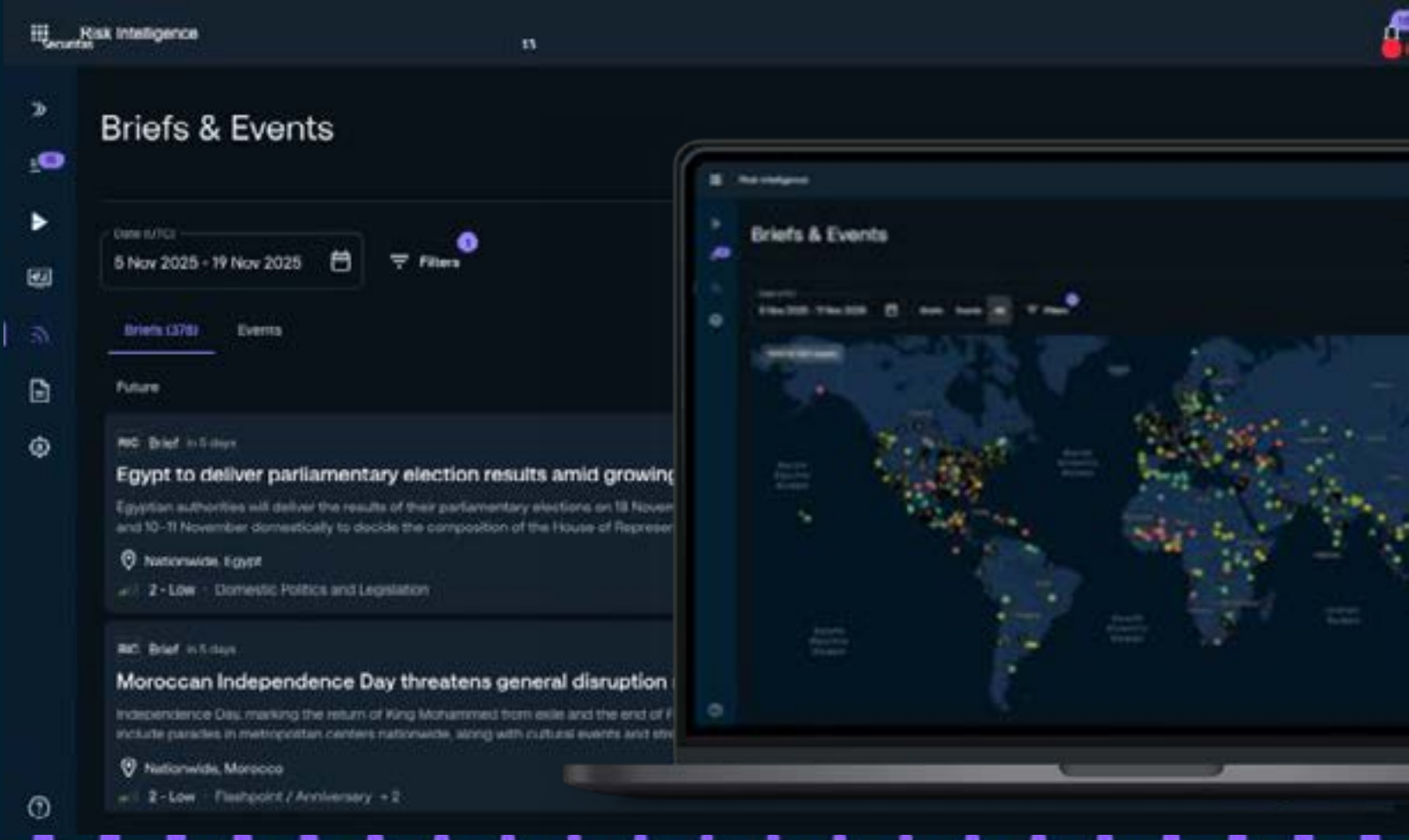
- Garantizar que los directivos de la organización realicen auditorías regulares de información personal pública y eliminar cualquier detalle que pueda ser usado.
- Monitorear las redes sociales para detectar cambios en la percepción en internet que puedan derivar en que los ejecutivos de la organización se conviertan en un objetivo.
- Garantizar que los planes de respuesta a incidentes estén en vigor y se pongan en práctica regularmente para abordar eficazmente los incidentes de doxxing, protegiendo a los ejecutivos de las organizaciones y a los centros de negocios.

Indicadores

- Las plataformas de redes sociales identificadas por tener una moderación de contenido débil o inconsistente.
- La creciente polarización de las plataformas de redes Sociales hacen que las plataformas se conviertan en ‘cámaras de eco’.
- Un aumento del activismo digital y el uso de las redes sociales para promover la ‘justicia social’.
- Aumento del acoso general y la persecución hacia organizaciones e individuos dentro de las plataformas de redes sociales.
- Mayor uso de redes de bots y sistemas impulsados por algoritmos para presentar y difundir misinformación, desinformación y malinformación.
- Publicación de bases de datos de directores generales y otros ejecutivos, especialmente para organizaciones sujetas a un mayor escrutinio público y descontento.

Implicaciones

- Los directivos de las organizaciones afrontan riesgos significativos para la seguridad personal si son atacados mediante una campaña masiva de doxxing.
- Las crecientes preocupaciones sobre la facilitación de campañas de doxxing a través de las redes sociales pueden llevar a regulaciones más estrictas y requisitos de cumplimiento para los sitios de redes sociales, especialmente en áreas como la privacidad de datos.
- Las organizaciones pueden estar obligadas a invertir en recursos de gestión de crisis para supervisar, identificar y responder a casos de doxxing de miembros ejecutivos.


Risk Intelligence
Briefs & Events
5 Nov 2025 - 19 Nov 2025
Filters
Briefs (378)
Events
Future
Brief
Egypt to deliver parliamentary election results amid growing
Nationwide, Egypt
2 - Low
Domestic Politics and Legislation
Brief
Moroccan Independence Day threatens general disruption
Nationwide, Morocco
2 - Low
Flashpoint / Anniversary
Briefs & Events

Global

2

Las quejas socioeconómicas compartidas impulsan la expansión de los movimientos de protesta de la ‘Generación Z’

En 2025 surgieron protestas antigubernamentales a gran escala, principalmente por jóvenes bajo el estandarte de la ‘Generación Z’, en varios países, incluyendo Argelia, Madagascar, México, Nepal y Perú, con manifestantes denunciando las malas condiciones económicas, la inestabilidad política y la corrupción gubernamental. Se espera que los éxitos de alto perfil de algunos de estos grupos, que implican la instigación de un cambio de régimen en ciertos casos, junto con factores socioeconómicos compartidos, fomenten la difusión e intensificación de

tales acciones de protesta a lo largo de 2026.

- Es muy probable que los países del Sur Global sigan viéndose especialmente afectados por futuras protestas, debido a que las condiciones en las regiones son propicias para el malestar estudiantil y juvenil provocado por agravios económicos y políticos.
- Los enfrentamientos violentos entre manifestantes y autoridades locales son muy probables de provocar interrupciones a nivel nacional y representan una amenaza para edificios oficiales y organizaciones con vínculos percibidos con el gobierno. Es muy probable que se usen banderas, lemas y el uso extensivo de símbolos juveniles para atraer a más participantes a unirse a las manifestaciones
- Es casi certero que el uso de las redes sociales casi con seguirá siendo una característica definitiva de las protestas de la ‘Generación Z’, permitiendo a los movimientos comunicarse y coordinar acciones de manera descentralizada, agravando las interrupciones a nivel nacional y comprometiendo la respuesta de las autoridades locales.

Escenario	Condición del escenario	Probabilidad evaluada
La tendencia de la ‘Generación Z’ se ralentiza, pero las protestas continúan ocurriendo con menos violencia y con menos enfrentamientos reportados con las fuerzas del orden.	Mejora	Altamente improbable (15%)
Las protestas continúan extendiéndose y atrayendo a una mayor participación, lo que provoca grandes cambios en el panorama político sin necesariamente satisfacer la totalidad de las quejas de los manifestantes.	Línea base	Posible / Probable (40%)
El éxito de las anteriores manifestaciones de la ‘Generación Z’ fomenta la formación de nuevos grupos. Las protestas violentas se han extendido a nivel global y ya agravan la inseguridad en las regiones experimentando inestabilidad.	Empeora	Improbable (45%)

Recomendaciones

- Mejorar la monitorización de las plataformas online utilizadas por los movimientos de la ‘Generación Z’ para coordinar sus actividades, incluyendo Discord, Facebook, Instagram, LinkedIn, Reddit, TikTok y X.
- Se aconseja a los equipos de seguridad implementar planes de respuesta de emergencia y reforzar los protocolos de seguridad para mantener las operaciones empresariales y garantizar la seguridad de sus activos y personal. La implementación de contingencias debe abordar acuerdos de trabajo flexibles, como el trabajo remoto.
- Las organizaciones deben mantener una comunicación clara con consulados y embajadas para mantenerse informadas sobre el desarrollo de la situación y evaluar la seguridad del entorno empresarial.

Indicadores	Implicaciones
— Los grupos de la ‘Generación Z’ continúan movilizándose en redes sociales a nivel mundial, con protestas a gran escala planificadas y promovidas con antelación. — Los grandes movimientos de protesta de la Generación Z’ provocan cambios políticos significativos. — Los líderes políticos promueven medidas de seguridad reforzadas, especialmente en los alrededores de edificios oficiales. — El actual panorama de disturbios en el país afectado está elevado, con manifestantes de diversos orígenes denunciando las políticas socioeconómicas. — Aumentan las críticas y represalias en línea hacia el gobierno.	— Debido a la gran asistencia y a los TTP utilizados, se espera que las protestas de la ‘Generación Z’ interrumpan las operaciones empresariales y las cadenas de suministro locales. — Un cambio político importante resultará en la enmienda de la legislación para las empresas que operan en el país afectado. — El aumento de las medidas de seguridad para las organizaciones ubicadas en zonas propensas a protestas resultará en altos costes económicos. — Los enfrentamientos violentos con las autoridades locales provocarán daños a la propiedad e infraestructuras y pondrán en peligro la seguridad de los activos de las organizaciones ubicadas en zonas propensas a protestas.

La política económica estadounidense sostiene la incertidumbre y el riesgo global

La inestabilidad del mercado global persistirá durante 2026 debido a las impredecibles políticas económicas estadounidenses, causando impactos en múltiples industrias, especialmente aquellas que se perciben como provocadoras del desequilibrio comercial, incluyendo el acero/aluminio, la automotora, la electrónica/tecnología, la confección, las tierras raras , la alimentación y la agricultura, y la farmacéutica. Un caso pendiente ante el Tribunal Supremo sobre el uso de la Ley de Poderes Económicos de Emergencia Internacional por parte de la administración Trump probablemente reducirá su capacidad para establecer restricciones arbitrarias; sin embargo, en este caso, los esfuerzos para aplicar gravámenes dirigidos, aunque limitados, mediante interpretaciones de la Ley de Comercio de 1974 o la Ley de Expansión Comercial de 1962, siguen siendo una posibilidad realista.

— Aunque el uso de la acción militar directa sigue siendo remoto, la retórica estadounidense en 2025 señaló que Estados Unidos consideró operaciones militares para ejercer influencia en lugares estratégicamente significativos (como Groenlandia o el Canal de Panamá) en respuesta a amenazas geoeconómicas percibidas por los adversarios.

— Las indicaciones de que Estados Unidos está considerando el uso de la fuerza o ejerciendo presión sobre no adversarios para mejorar su posición estratégica inducirán un sentimiento negativo significativo del mercado y alejarán a los aliados estadounidenses existentes.

— Las organizaciones que buscan mitigar la incertidumbre pueden crear una mayor inestabilidad de mercado mediante medidas como el almacenamiento de materiales, la deslocalización cercana o desconectada y la revisión de la logística y las relaciones en la cadena de suministro. Enfoques como la mayor digitalización y centralización conllevan sus propios riesgos, como una mayor exposición a amenazas de ciberseguridad.

Escenario	Condición del escenario	Probabilidad evaluada
Estados Unidos mantiene restricciones específicas con límites impuestos por los tribunales, lo que mantiene un sentimiento negativo del mercado, aunque con objetivos más predecibles y estrechos.	Mejora	Altamente improbable (55%)
Estados Unidos sigue imponiendo restricciones de manera impredecible y arbitraria, como castigar desacuerdos políticos con socios comerciales, lo que obliga a los aliados estadounidenses a explorar socios comerciales alternativos para asegurar la adquisición de bienes clave.	Línea base	Posible / Probable (40%)
Estados Unidos lleva a cabo operaciones militares para tomar el control de puntos estratégicos económicos, empeorando la inestabilidad económica global y la seguridad regional.	Empeora	Remoto (5%)

Recomendaciones

— Considerar desarrollar planes de escalada para orientar la toma de decisiones en medio de regulaciones que cambian rápidamente, teniendo en cuenta la continuidad operativa en las regiones afectadas.

— Auditar / introducir estrategias de prevención y mitigación de pérdidas, especialmente para organizaciones con cadenas de suministro globales.

— Las organizaciones implicadas en la logística de la cadena de suministro deberían considerar revisar los impactos en las operaciones basándose en la pérdida de servicios prestados por empresas centradas en EE. UU. (incluidos sistemas basados en IA y GPS).

Indicadores	Implicaciones
— El Tribunal Supremo emite una sentencia a principios de 2026 limitando la autoridad del Ejecutivo para establecer aranceles y controles de exportación. — La Casa Blanca ordena al Secretario de Comercio que realice investigaciones bajo la Ley de Expansión Comercial. — Creciente retórica política de la administración estadounidense en torno a la toma y control de áreas estratégicas clave. — Los acuerdos bilaterales entre aliados de EE. UU. (por ejemplo, Europa Occidental, Canadá) se profundizan con China y potencias medias (por ejemplo, Colombia). — Soluciones de mercado habilitadas por IA que buscan abordar los desafíos de la cadena de suministro surgen rápidamente.	— Las fluctuaciones en los costos afectan a las previsiones financieras y valoraciones empresariales. — Los mercados se vuelven cada vez más oportunistas o inviables, lo que provoca la reubicación de las operaciones empresariales. — Mayor gasto para mitigar vulnerabilidades de seguridad debido a procesos y protocolos nuevos o desconocidos. — La política estadounidense provoca que determinadas industrias u organizaciones sufran pérdidas financieras debido a infracciones de cumplimiento. — Las empresas experimentan una amenaza interna pronunciada, especialmente si operan en sectores críticos.

La proliferación de material terrorista en plataformas abiertas impulsa amenazas terroristas autoinducidas

El contenido extremista, los manifiestos terroristas y la propaganda ideológica se seguirán proliferando en línea durante todo 2026, incluyendo redes sociales convencionales, plataformas de videojuegos y sitios descentralizados de intercambio de archivos. Este contenido permitirá que terroristas autoiniciados (S-ITs) —individuos sin vínculos formales con grupos terroristas establecidos— planifiquen y lleven a cabo ataques con poco o ningún apoyo externo. El fácil acceso a directrices detalladas sobre la planificación de ataques y la selección de objetivos, junto con la disponibilidad de tecnologías emergentes como drones e impresoras 3D, impulsará cambios continuos en el panorama de amenazas para la seguridad física.

- Es casi certero que Los S-IT seguirán siendo el vector de amenaza más difícil de monitorizar eficazmente para los servicios de seguridad, dada su falta de vínculos con redes establecidas y su huella digital mínima. Los S-IT suelen replicar tácticas, técnicas y procedimientos (TTP) disponibles en manuales de circulación pública, especialmente ataques de baja complejidad como embestir vehículos, ataques cuerpo a cuerpo y asaltos con armas ligeras.
- La creciente politización y fragmentación de las plataformas de redes sociales, combinada con la incapacidad de la moderación de contenidos para mantenerse al día, creará condiciones ideales para que los usuarios de redes sociales se radicalicen a sí mismos.
- Los grupos extremistas ya están experimentando con el uso de herramientas de IA generativa, lo que indica el potencial de explotación a medio y largo plazo. Es muy probable que la IA se utilice para eludir los sistemas existentes de moderación de contenido y explotar crisis mediante la rápida creación y difusión de propaganda para incitar a la violencia.

Escenario	Condición del escenario	Probabilidad evaluada
La difusión de material extremista abiertamente accesible disminuye debido a una mejor moderación de contenido, lo que ralentiza el camino hacia la auto-radicalización y obliga a posibles extremistas a adoptar vías establecidas (y monitorizadas).	Mejora	Altamente improbable (10%)
Los ataques S-IT persisten en los niveles actuales, ya que el contenido extremista sigue siendo accesible en plataformas públicas, permitiendo que las personas se radicalicen de forma independiente.	Línea base	Posible / Probable (55%)
El volumen y la sofisticación de materiales terroristas accesibles al público de manera significativa incrementa, impulsando un auge de tramas autoiniciadas a nivel mundial.	Empeora	Improbable (35%)

Recomendaciones

- Desarrollar planes de escenarios para tipos comunes de ataques terroristas, incluyendo escenarios de ataque que involucren armas cuerpo a cuerpo, explosivos, armas de fuego, fuego como arma, vehículos como armas, secuestro, rescate-extorsión y sustancias nocivas, incluyendo químicas, biológicas, radiológicas y nucleares (CBRN).
- Garantizar que el personal esté al tanto de los signos y procesos para denunciar a personas potencialmente radicalizadas y proporcionar formación y herramientas para facilitar y apoyar a los empleados.
- Implementar procesos de monitorización y alerta para identificar y verificar posibles incidentes de amenaza a través del personal sobre el terreno, las noticias locales y las redes sociales, corroborando cualquier información con fuentes oficiales o creíbles.

Indicadores	Implicaciones
— Las agencias de seguridad nacional emiten alertas / elevan los niveles de terrorismo advirtiendo sobre el aumento de amenazas autoiniciadas relacionadas con la radicalización en línea. — Expansión de contenido propagandístico dirigido a grupos regionales o demográficos previamente inexplorados (es decir, propaganda traducida a diferentes idiomas). — Aumento sustancial en los compartidos, descargas o republicaciones de manuales y propaganda extremistas en plataformas de código abierto. — Plataformas tecnológicas disolviendo equipos de moderación de contenido o cambiando sus políticas, permitiendo que más contenido extremista quede sin control.	— Las organizaciones en las principales áreas metropolitanas experimentan interrupciones operativas debido a niveles elevados de amenaza y medidas de seguridad reforzadas. — El perfil objetivo de los S-IT se amplía a medida que el contenido extremista en línea interactúa con agravios personales, con posibles objetivos como organizaciones privadas. — Las empresas son más propensas a sufrir daños reputacionales y posibles acciones regulatorias si sus servicios, plataformas o productos son explotados para producir, alojar o distribuir materiales terroristas.

AMEA

El panorama de seguridad en Oriente Medio se complica tras el alto el fuego en Gaza

Los principales acontecimientos en Oriente Medio continuaron agravando la incertidumbre regional en 2025, agravados por el colapso del primer alto el fuego Gaza-Israel en marzo; el conflicto Irán-Israel de 12 días en junio; y el cese de las negociaciones nucleares entre Irán y Estados Unidos. Aunque un segundo alto el fuego en Gaza está en vigor desde octubre, las tensiones en Oriente Medio siguen estando elevadas, con poca resolución a la vista para muchos de los principales motores de tensiones regionales al comenzar 2026.

— Mientras Estados Unidos y otros estados buscan establecer una fuerza de tarea internacional en Gaza para apoyar la post-gobernanza y estabilidad del conflicto, es probable que Israel exprese su oposición a la implicación de ciertos estados, especialmente Turquía, preservando los desacuerdos sobre la futura administración del territorio.

— Tras sufrir considerables pérdidas durante conflictos directos y por poder con Israel en 2025, Irán y sus grupos aliados probablemente buscarán regenerar y renovar su capacidad, con el objetivo de volver a los objetivos y tácticas estratégicas anteriores. Aunque la influencia generalizada probablemente será un reto en 2026 debido a la magnitud de las pérdidas, los ataques a los puntos estratégicos clave y los objetivos ideológicos (como las acciones en la frontera yemení) casi con toda seguridad persistirán.

— Las negociaciones nucleares entre Irán y Estados Unidos siguen estancadas, con pocas señales de progreso. Sin un camino inmediato hacia un acuerdo, las tensiones bilaterales casi con toda seguridad seguirán elevadas durante todo 2026, manteniendo riesgos para los activos occidentales derivados de operaciones iraníes de guerra en la zona gris (GZW), como ciberataques.

Escenario	Condición del escenario	Probabilidad evaluada
Se establece un acuerdo de paz a largo plazo en Gaza. La mejora de las relaciones entre Israel y Estados Unidos con Irán y Siria llevó a acuerdos formales de seguridad, desescalando el panorama de seguridad.	Mejora	Altamente improbable (10%)
Pocos avances en las negociaciones nucleares entre Irán y Estados Unidos, con enfrentamientos aislados en la región de Oriente Medio (Gaza, Líbano, Siria) que amenazan con un nuevo conflicto cinético y con mayor incertidumbre.	Línea base	Posible / Probable (50%)
Conflicto cinético renovado en escenarios separados que involucran a Israel (Gaza, Irán, Líbano, Siria), lo que resultó en un nuevo ataque al tráfico marítimo en el Mar Rojo, interrumpiendo operaciones comerciales	Empeora	Improbable (40%)

Recomendaciones

— Desarrollar planes detallados de continuidad del negocio que tengan en cuenta diversos escenarios de interrupción, incluyendo el cierre de rutas marítimas, las interrupciones bancarias regionales y las interrupciones de la cadena de suministro a nivel local, regional y global.

— Revisar y mejorar las medidas de ciberseguridad para proteger contra ataques patrocinados por el Estado, centrándose especialmente en infraestructuras críticas y datos sensibles.

— Mantener la conciencia sobre el potencial de las tensiones en Oriente Medio para seguir motivando a actores amenazantes a nivel internacional, incluidos activistas y terroristas / extremistas.

Indicadores

- Aumento de incidentes en Gaza / Líbano que involucran fuerzas militares israelíes y proxies iraníes como Hamás / Hezbolá.
- Un fuerte aumento de incidentes de seguridad marítima en el Mar Rojo y el Golfo Pérsico, especialmente en los que involucran embarcaciones vinculadas a intereses israelíes o occidentales.
- Cambios repentinos en los movimientos o despliegues de tropas israelíes en Gaza, Líbano y Siria.
- Colapsos en las conversaciones sobre el grupo de trabajo internacional en Gaza y su gobernanza posconflicto.
- Escaladas en las tensiones israelíes con Siria e Irán, incluyendo un aumento de la retórica entorno a Gaza.

Implicaciones

- Cambios rápidos en la dinámica regional como resultado de cambios de lealtades, como las relaciones de Estados Unidos con Israel / Siria.
- La reaparición de disrupciones en las cadenas de suministro regionales y en las rutas de transporte marítimo, con un impacto particular en los sectores energético y marítimo.
- Crecimiento en la frecuencia / intensificación de las actividades por parte del movimiento global pro-Palestina, que supone amenazas para organizaciones occidentales con vínculos reales o percibidos con Israel.
- Cambio estratégico requerido en las operaciones empresariales debido a los desarrollos regionales que generan nuevas dinámicas de seguridad.

Militantes islamistas amplían su actividad en África Occidental

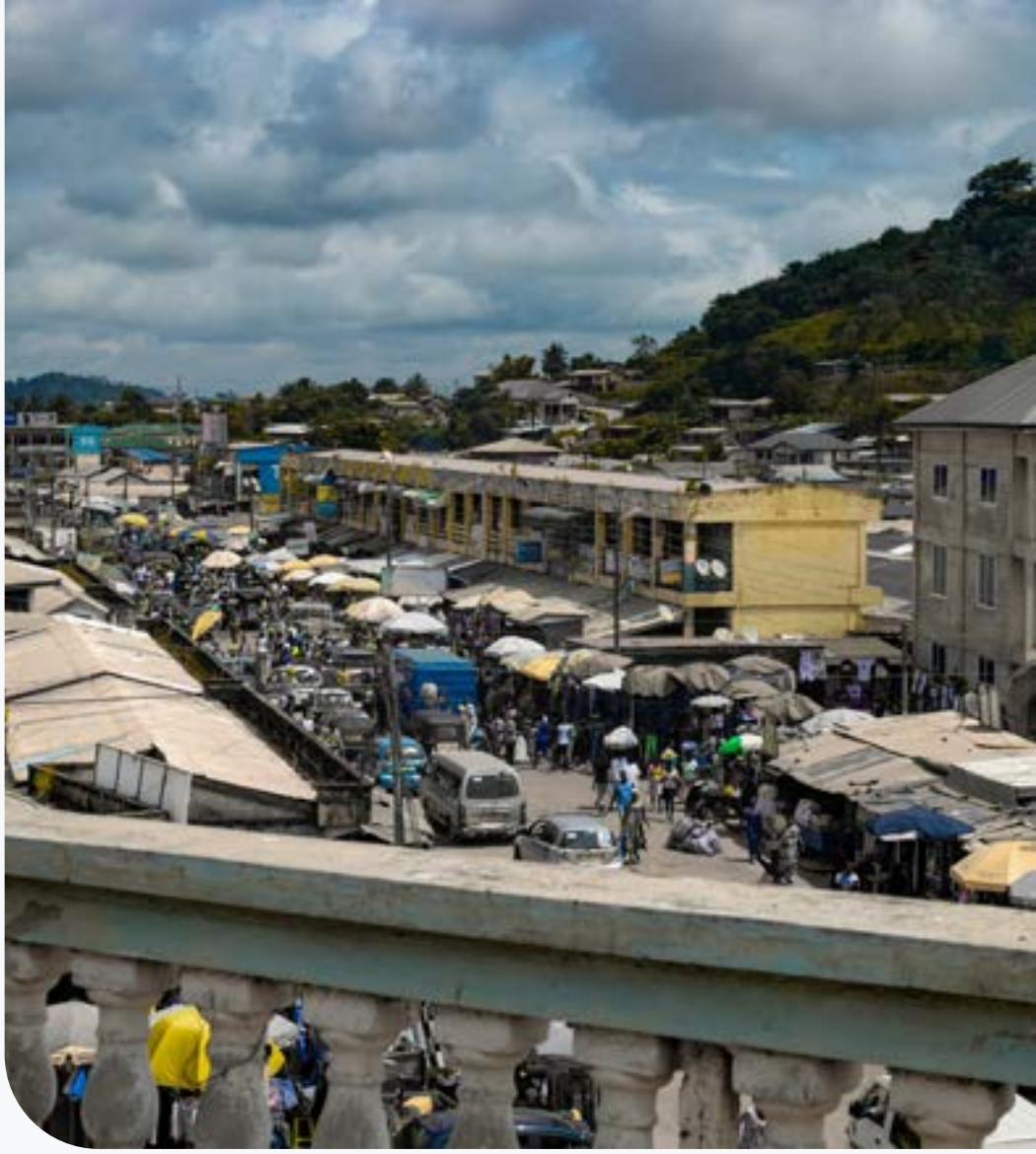
Diversos grupos islamistas, incluidos Boko, Haram y la provincia del Estado Islámico de África Occidental, continuaron intensificando los ataques en el Sahel y África Occidental en 2025, dirigiéndose a civiles, personal militar, instituciones gubernamentales y activos empresariales. Países como Burkina Faso, Níger y Malí seguirán sintiendo los efectos de la retirada del apoyo militar occidental a las operaciones antiterroristas. Es probable que Malí siga experimentando la escalada más pronunciada, impulsada por la creciente influencia de Jama'at Nusrat ul-Islam wa al-Muslimin (JNIM), que ha interrumpido las cadenas de suministro de combustible entre Senegal y la capital maliense, Bamako, a finales de 2025.

- Es probable que los estados afectados se enfrenten a un creciente aislamiento internacional, ya que gobiernos extranjeros emiten avisos de viaje para proteger a los nacionales. Esto probablemente agravará las dificultades económicAs, ralentizará la inversión y el crecimiento, y afianzará aún más a los grupos extremistas, especialmente en zonas remotas, donde los esfuerzos antiterroristas siguen siendo insuficientes.
- Los grupos islamistas, especialmente el JNIM, probablemente llevarán a cabo cada vez más operaciones transnacionales, explotando zonas con débil control gubernamental para lanzar ataques a través de las fronteras y potencialmente en el extranjero. Estos esfuerzos probablemente se verán reforzados por el creciente uso de tecnologías avanzadas, como drones, por parte de los grupos para llevar a cabo ataques.
- Los ataques contra inversiones extranjeras, operaciones mineras e infraestructuras críticas probablemente se intensificarán, incluyendo potencialmente campañas coordinadas de extorsión, operaciones de secuestro a cambio de rescate e interrupciones deliberadas de las cadenas de suministro regionales que conectan estados sin salida al mar del Sahel con puertos costeros.

Escenario	Condición del escenario	Probabilidad evaluada
Los estados regionales, junto con socios internacionales, lanzan operaciones antiterroristas a nivel regional, desplazando a grupos a zonas cada vez más remotas.	Mejora	Altamente improbable (10%)
Los grupos islamistas continúan lanzando ataques; sin embargo, siguen siendo amenazas internas dentro de países individuales o en áreas geográficas confinadas. Las regiones siguen siendo hostiles hacia los extranjeros y las empresas.	Línea base	Posible / Probable (40%)
Los grupos islamistas continúan intensificando y ampliando los ataques a través de las fronteras, presentándose crecientes amenazas a la estabilidad política / activos extranjeros, e intereses en toda la región	Empeora	Improbable (50%)

Recomendaciones

- Supervisar las recomendaciones gubernamentales y las declaraciones públicas, incluyendo restricciones a regiones y subregiones específicas, despliegues de seguridad y precauciones de seguridad como avisos de confinamiento en casa.
- Para empresas que operan en regiones volátiles, implementar medidas sólidas de seguridad y protección de personal, así como planes de contingencia / de continuidad en caso de objetivo.
- Desarrollar y mantener planes de comunicación con el personal de regiones volátiles para asegurar la rápida notificación de avisos y cambios en las medidas de seguridad.



Indicadores	Implicaciones
— Los ataques aumentan en frecuencia y gravedad dirigiéndose cada vez más a áreas de población más amplias. — Comienzan a ocurrir ataques en regiones o estados previamente no afectados — Aumentan los secuestros, rescates y extorsiones de extranjeros. — Aumento de las restricciones de movilidad y las interrupciones en la cadena de suministro atribuidas a grupos extremistas. — Los gobiernos regionales organizan reuniones para planificar acciones coordinadas contra el terrorismo. — Más avisos de viaje a gobiernos extranjeros que también comienzan a incluir a países vecinos.	— Los disturbios internos se intensifican en las regiones afectadas, lo que provoca protestas y enfrentamientos violentos en las zonas urbanas. — Las cadenas de suministro críticas de minerales de las regiones se ven interrumpidas, afectando las operaciones de los sectores dependientes. — Los desafíos humanitarios se intensifican en las regiones afectadas, incluyendo hambrunas, brotes de enfermedades y acceso restringido a suministros de ayuda crítica. — Los ciudadanos extranjeros enfrentan mayores amenazas a la seguridad, con riesgos extendidos a expatriados, personal diplomático y empresarios.

Los mercados emergentes presentan oportunidades y riesgos para las empresas

La reducción o finalización de los conflictos en la región AMEA a lo largo de 2025 ha abierto oportunidades para una reanudación de la participación del sector privado. La reintegración de Siria a la comunidad internacional y a la economía global bajo el nuevo régimen del presidente Ahmed al-Sharaa constituye el ejemplo más significativo; no obstante, el alto el fuego en Gaza, la disminución de la intensidad del conflicto o un alto el fuego limitado en Myanmar, el desarme del Partido de los Trabajadores del Kurdistán (PKK), así como los acuerdos de paz en la República Democrática del Congo (RDC) y entre Armenia y Azerbaiyán, también podrían generar oportunidades en 2026.

— El acceso a mercados previamente inaccesibles y a los lucrativos contratos de reconstrucción y desarrollo probablemente fomentará la dirección extranjera directa la inversión (IED), que, junto con la ayuda estatal extranjera, la eliminación de sanciones y el retorno de capital humano del extranjero, tiene el potencial de mejorar las condiciones humanitarias y fomentar el crecimiento económico.

— A pesar de que los conflictos se están desescalando, la situación de seguridad sigue siendo frágil en muchos casos. Los riesgos incluyen que los excombatientes recurran a la criminalidad o realicen ataques de venganza para socavar a las autoridades, tensiones sociopolíticas persistentes que obstaculicen el desarrollo y la reconstrucción, o que el conflicto se vuelva a escalar en respuesta a un punto conflictivo.

Escenario	Condición del escenario	Probabilidad evaluada
La rápida mejora económica en los países posconflicto se impulsa gracias a una reconciliación positiva entre facciones previamente competidoras y al apoyo financiero significativo de socios internacionales.	Mejora	Altamente improbable (10%)
El alto el fuego / cese de conflictos se mantiene con niveles moderados de problemas de seguridad residual. La reconstrucción económica avanza gradualmente, pero se ve temperada por tensiones persistentes.	Línea base	Posible / Probable (50%)
El conflicto se reactiva con nuevas facciones rivales dentro del régimen gobernante que toman se rebelar, o rivales anteriores que eligieron volver al conflicto o involucrarse en la violencia insurgencia.	Empeora	Improbable (40%)

Recomendaciones

— Las empresas que consideren reabrir mercados deben realizar una rigurosa debida diligencia y evaluaciones de riesgos para operar en el país y crear planes de contingencia sólidos para una variedad de posibles problemas de seguridad.

— Contratar a nacionales locales verificados y de confianza para navegar las complejidades del estado posconflicto. Estos deberían incluir tanto a personas que permanecieron en el país durante el conflicto, a los refugiados que huyeron de los combates como a los ciudadanos con doble nacionalidad familiarizados con el idioma y la cultura tanto del país anfitrión como de la empresa implicada.

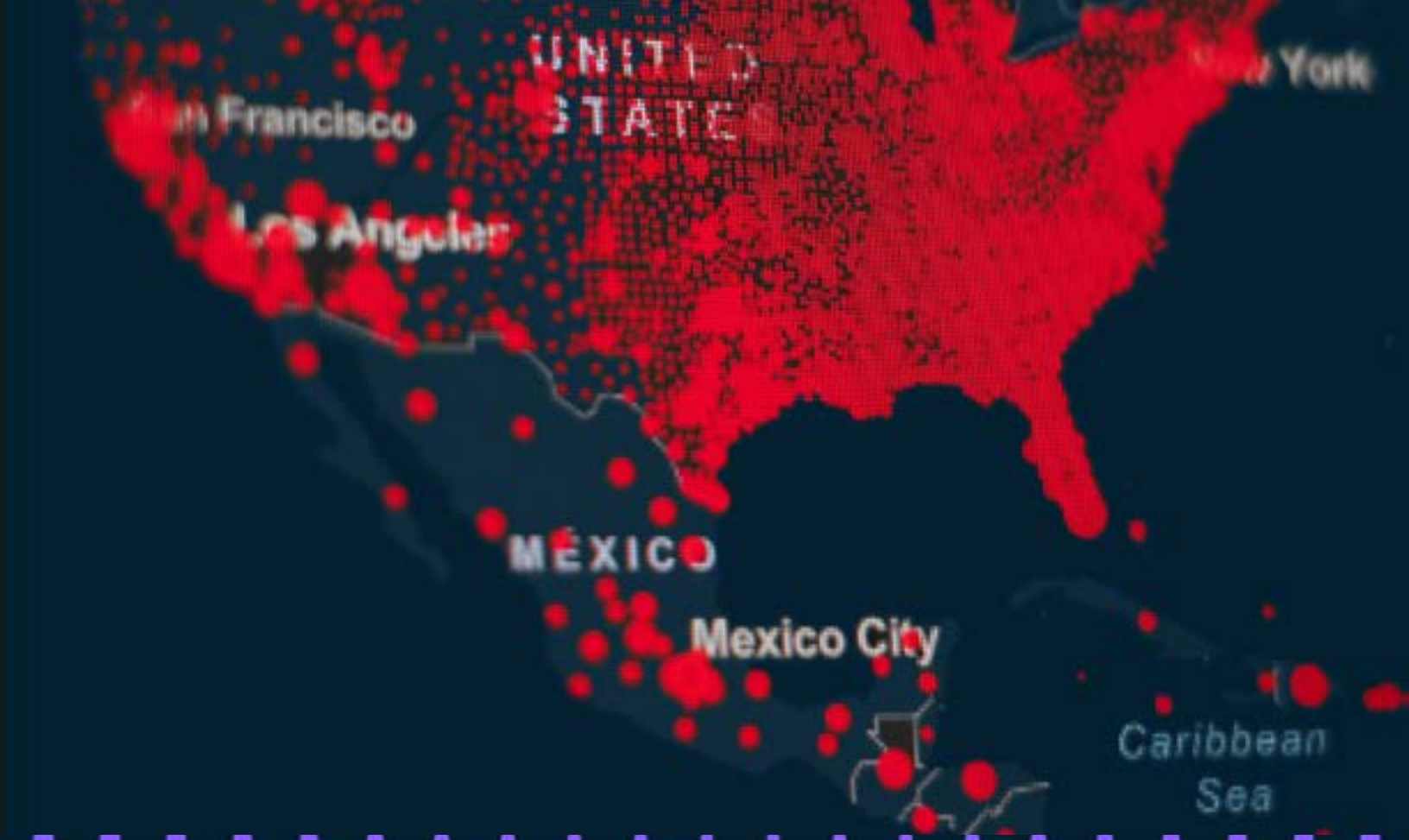
— Invertir en medidas de seguridad adecuadas y multinivel, que incluyan personal local de confianza, equipos internos de seguridad física e inteligencia, y canales de coordinación establecidos con actores clave, como fuerzas de mantenimiento de la paz y agregados de embajadas.

Indicadores

- Implicación sostenida de bloques geopolíticos clave en las negociaciones entre partes involucradas en conflicto.
- Restablecimiento formal de relaciones diplomáticas y reapertura de embajadas por parte de los principales estados.
- Suspensión o alivio de sanciones y aranceles para los países implicados en conflictos
- Organizaciones que expanden sus operaciones a áreas previamente afectadas por conflictos.
- Mayor tasa de retorno de refugiados a los países afectados.

Implicaciones

- La reintegración de múltiples países o áreas en la economía global probablemente cambiará las cadenas de suministro y presentará oportunidades económicas lucrativas.
- Las organizaciones que invierten fuertemente en mercados emergentes tienen muchas probabilidades de enfrentarse a una exposición significativa en caso de que el conflicto se reanude o la situación de seguridad se desestabilice.
- Las empresas que cooperan estrechamente con nuevas autoridades o con una sola facción corren el riesgo de ser vistas como un objetivo legítimo en los combates residuales.
- Las tendencias migratorias invertidas podrían generar nuevas tensiones en cuestiones como la propiedad de la tierra.



América

4

La reorientación de Estados Unidos hacia América Latina agrava la incertidumbre política y la inestabilidad regional

La reorientación de la política exterior de Estados Unidos hacia América Latina (LATAM) tras el regreso de Donald Trump a la presidencia se prevé que continúe en 2026. Si bien este enfoque estuvo inicialmente dirigido a contrarrestar las operaciones de narcotráfico de los grupos de crimen organizado (OCG), desde entonces ha evolucionado hacia un esfuerzo por reafirmar la influencia estadounidense en la región, convirtiéndose en un factor significativo de incertidumbre política e inestabilidad regional. La renovada implicación de EE. UU. en LATAM es muy probablemente una respuesta a la creciente preocupación por el aumento de la influencia política y económica de China en la región.

— Estados Unidos lanzó ataques aéreos contra objetivos terrestres en Venezuela y detuvo al presidente Nicolás Maduro durante una operación llevada a cabo en la madrugada del 3 de enero. Desde entonces, el presidente estadounidense Donald Trump ha indicado que EE. UU. supervisará una transición de poder en el país y ha amenazado con nuevas acciones si las autoridades nacionales no cooperan; sin embargo, los planes de transición no han sido divulgados públicamente en detalle y la situación continúa siendo volátil.

— La reactivación y modernización de instalaciones militares estadounidenses en el Caribe tiene el potencial de facilitar el despliegue a largo plazo de capacidades militares avanzadas. Es altamente probable que los países de LATAM perciban esto como una amenaza a la seguridad, lo que podría derivar en un fortalecimiento de los vínculos económicos y militares con rivales estratégicos de EE. UU.

— Es probable que Estados Unidos intensifique las operaciones de guerra de zona gris (GZW) en LATAM, particularmente en países percibidos como “no alineados” o “hostiles” a los intereses estadounidenses. La administración Trump ha demostrado disposición a forzar cambios de régimen, y el uso de retórica incendiaria para influir en la política exterior casi con certeza incrementará la polarización política en América Latina.

Escenario	Condición del escenario	Probabilidad evaluada
Estados Unidos coopera con las autoridades nacionales para supervisar una transición de poder pacifica y ordenada en Venezuela y reduce su acumulación de presencia militar en el Mar Caribe	Mejora	Altamente improbable (10%)
La situación en Venezuela sigue siendo inestable y volátil ya que los detalles acerca de la transición de poder dirigida por los Estados Unidos siguen siendo poco claros. De manera paralela, EE.UU. mantienen la presión de regímenes en países como Colombia y Cuba.	Línea base	Posible / Probable (65%)
El panorama de seguridad de Venezuela se deteriora mientras las facciones rivales intentan afirmar la situación empeora autoridad sobre el país, mientras que Estados Unidos toma medidas adicionales contra el liderazgo de regímenes adversarios	Empeora	Improbable (25%)

Recomendaciones

— Evaluar la exposición / dependencia de las cadenas de suministro / rutas comerciales de regiones específicas, con el objetivo de diversificar y minimizar las interrupciones causadas por eventos geopolíticos.

— Desarrollar planes de contingencia para relaciones diplomáticas interrumpidas, periodos intensificados de amenazas o disturbios e invertir en servicios de inteligencia de riesgos geopolíticos para supervisar, anticipar y responder a conflictos en desarrollo.

— Desarrollar planes detallados de continuidad del negocio que tengan en cuenta diversos escenarios de interrupción, incluyendo el cierre de rutas marítimas, las interrupciones bancarias regionales y la interrupción de la cadena de suministro, tanto para empresas de la región como a nivel internacional.

Indicadores

- La continua modernización y reacondicionamiento de la infraestructura militar estadounidense en el Caribe, como bases aéreas e instalaciones navales, junto con despliegues adicionales de equipamiento militar avanzado en la región.
- Aumento de mensajes antiestadounidenses en varios países de LATAM y viceversa en Estados Unidos.
- Manifestaciones en países de LATAM, citando el 'imperialismo estadounidense', exigiendo el cese de la interferencia estadounidense en asuntos internos y la ruptura de los lazos con Estados Unidos.
- Anuncios de mayor cooperación / acuerdos entre estados de LATAM y rivales estratégicos estadounidenses
- Cambios en la elección de la política estadounidense para llevar a cabo acciones directas en ciertos países de LATAM.

Implicaciones

- Mayor complejidad de cumplimiento para las corporaciones multinacionales que operan en jurisdicciones de LATAM y Estados Unidos.
- Aumento del panorama de protestas / acción directa dirigida contra organizaciones vinculadas a Estados Unidos por grupos activistas pro-LATAM / anti-EE. UU., afectando negativamente las operaciones de la organización.
- La incertidumbre regional socava la confianza de los inversores, reduciendo la inversión extranjera.
- Deterioro de las relaciones diplomáticas, incluso entre aliados de larga duración, lo que provoca obstrucciones a los viajes de los empleados y al comercio bilateral.

El extremismo político crece en alcance y frecuencia en Estados Unidos

Los actos de extremismo político han aumentado significativamente en Estados Unidos en los últimos dos años, impulsados por la ampliación de las divisiones políticas existentes y la mayor prevalencia y acceso a opiniones políticas de extrema izquierda/derecha en toda la sociedad estadounidense. Los entornos de redes sociales cada vez más poco moderados y partidistas están llevando a que las personas se radicalicen cada vez más por sí mismos o externamente, y con la administración actual sin mostrar señales de retroceder en sus políticas y retórica más divisivas, es muy probable que se produzcan más actos de extremismo motivado políticamente en 2026.

— El uso de Inmigración y Control de Aduanas (ICE) y otras agencias para combatir la inmigración ilegal, los recortes a los departamentos federales y los impactos económicos de los aranceles comerciales globales continuará} para impulsar la polarización política. Es muy probable que los grupos activistas y extremistas sigan centrándose en estos temas y en quienes los promuevan, implementan o apoyan.

— Es probable que los 'días de acción' a nivel nacional en oposición a la política gubernamental continuarán, proporcionando puntos conflictivos y plataformas para un posible extremismo político tanto por parte de manifestantes anti-Trump como de contra-manifestantes.

— Acciones extremas como asesinatos y actos de sabotaje, violencia y vandalismo grave casi con toda seguridad seguirán siendo planificadas, impulsadas tanto por la retórica inflamatoria como por la formulación de políticas altamente divisiva y la creciente normalización de puntos de vista extremos tanto en los medios convencionales como en los alternativos.

Escenario	Condición del escenario	Probabilidad evaluada
Las políticas y discursos divisivos de figuras políticas se reducen en un intento por mitigar respuestas extremistas. Asimismo, mejora la moderación de los medios de comunicación tradicionales y alternativos, disminuyendo la exposición de las personas a contenidos e ideologías extremistas.	Mejora	Remoto (5%)
La polarización política se mantiene en los niveles actuales, continuando el impulso al extremismo político tanto desde actores de izquierda y derecha como desde grupos marginales.	Línea base	Posible / Probable (70%)
La administración Trump redobla su apuesta por políticas de línea dura en áreas divisivas como la inmigración. De forma paralela, un número creciente de grupos activistas es catalogado como entidades "terroristas", lo que empuja a estos actores a la clandestinidad y eleva el riesgo de radicalización y de acciones extremistas.	Empeora	Improbable (25%)

Recomendaciones

— Mantener monitoreo permanente del entorno de protestas y manifestaciones que puedan servir como plataforma para el extremismo político, especialmente durante periodos de mayor actividad política, como las elecciones de medio término de 2026.

— Evaluar los portafolios y activos para identificar elementos que puedan ser percibidos como vinculados a un partido, grupo o política específica y que, por ello, puedan convertirse en objetivos de actores extremistas.

— Se recomienda que las organizaciones mantengan un conocimiento sólido y actualizado sobre las tácticas, técnicas y procedimientos (TTPs) empleados por extremistas políticos que hayan ejecutado o intentado llevar a cabo acciones de amenaza.

Indicadores

- Las figuras políticas dentro de la política convencional continúan vocalizando y difundiendo retórica extremista.
- Persiste un panorama de protestas elevado, con eventos simbólicos, como festivos federales, que actúan como puntos de conflicto para el descontento.
- Se promulgan o refuerzan políticas controvertidas o divisivas a pesar de la reacción política y pública
- La administración Trump implementa medidas para proteger los activos federales contra la violencia política.
- Los grupos activistas se designan como organizaciones terroristas', y la designación se utiliza para facilitar la acción policial.

Implicaciones

- Las organizaciones con vínculos percibidos con iniciativas políticas sufren amenazas de seguridad relacionadas con el extremismo político.
- El aumento de la polarización política y la radicalización incrementarán el riesgo de incidentes de amenazas internas, especialmente en organizaciones cercanas a temas divisivos.
- La confianza extranjera en el panorama empresarial estadounidense probablemente se degradará mientras que el extremismo político siga siendo alto.
- Los adversarios extranjeros tienen muchas probabilidades de aprovechar la normalización del extremismo político para dirigirlo hacia empresas en sectores estratégicamente importantes.

Estados Unidos cambia de enfoque de ‘Guerra contra el Terrorismo’ a ‘Guerra contra el Crimen’

La administración Trump ha desplazado las operaciones militares estadounidenses de la lucha contra el terrorismo hacia la lucha contra el crimen en los últimos meses de 2025. Es muy probable que este enfoque continúe o se intensifique hasta principios de 2026. Mientras que antes el ejército estadounidense adoptaba un enfoque de contrainsurgencia con la guerra contra el terrorismo, la administración Trump utiliza cada vez más designaciones terroristas para atacar a grupos criminales y a aquellos percibidos como adversarios de los objetivos del gobierno estadounidense. Esto incluye designar varios cárteles de droga en América Latina como organizaciones terroristas extranjeras (FTOs), así como grupos o filosofías de izquierdas extranjeras y nacionales, incluyendo Antifa en EE. UU. y Antifa Ost en Alemania.

- La designación de grupos criminales extranjeros y nacionales como FTOs permite a la administración Trump modificar su enfoque al atacar a estos grupos, facilitando el uso de capacidades militares contra objetivos estratégicos.
- Aunque la administración Trump ha demostrado su intención de invertir recursos en la lucha contra el crimen en Estados Unidos, esto ha provocado un aumento de ataques contra grupos de crimen organizado extranjeros, muchos de los cuales ahora son FTOs, así como un incremento de las represiones contra grupos de protesta de la oposición. Ambos otorgan a Estados Unidos acceso a capacidades reforzadas para atacar adversarios extranjeros considerados cómplices en actividades criminales, incluidos gobiernos extranjeros.
- Trump probablemente seguirá intentando emplear a la Guardia Nacional de EE. UU. para complementar las capacidades de lucha contra el crimen y las fuerzas del orden en ciudades de todo Estados Unidos. Si estos despliegues escalaran hasta convertirse en ataques nacionales o internacionales, es muy probable que desencadenaran desafíos legales y constitucionales.

Escenario	Condición del escenario	Probabilidad evaluada
El gobierno de Estados Unidos reduce el uso de designaciones terroristas para atacar a grupos criminales y activistas. Aunque algunos grupos criminales están designados como FTOs, la actividad militar estadounidense sigue siendo limitada.	Mejora	Altamente improbable (10%)
La administración Trump sigue designando a grupos criminales extranjeros como FTOs para facilitar el uso de fuerzas militares contra grupos nacionales designados como tales.	Línea base	Posible / Probable (70%)
La criminalización generalizada de grupos y activistas de la oposición conduce a la despliegue de activos militares tanto a nivel nacional como internacional, fomentando disturbios y desafíos legales.	Empeora	Improbable (20%)

Recomendaciones

- Evaluar la exposición / dependencia de las cadenas de suministro / rutas comerciales de regiones específicas, con el objetivo de diversificar y minimizar las interrupciones causadas por eventos geopolíticos.
- Desarrollar planes de contingencia para relaciones diplomáticas interrumpidas, periodos intensificados de amenazas o disturbios e invertir en servicios de inteligencia de riesgos geopolíticos para supervisar, anticipar y responder a conflictos en desarrollo.
- Mantener la conciencia de las relaciones políticas internas y exteriores, ya que la política estadounidense y la administración Trump pueden afectar tanto al entorno comercial interno como exterior.

Indicadores
— Continuidad de la designación de grupos criminales extranjeros como FTOs, dando precedente para que el gobierno de EE. UU. implemente designaciones similares en grupos nacionales. — La administración Trump sigue utilizando la Guardia Nacional para contrarrestar las protestas antigubernamentales, publicando narrativas que piden la criminalización de grupos activistas de izquierdas. — El uso creciente de retórica cada vez más incendiaria entre políticos republicanos y demócratas conduce a una mayor atribución de culpas por los desafíos internos. — Los ataques violentos perpetrados por organizaciones criminales extranjeras están siendo percibidos como actividad terrorista, lo que permite al gobierno aplicar designaciones formales.

Implicaciones
— Un entorno social cada vez más restrictivo, donde la oposición política está cada vez más criminalizada. — Las organizaciones con operaciones en el extranjero se verán cada vez más afectadas por sentimientos negativos hacia el gobierno de EE. UU. — Los grupos criminales extranjeros, aquellos con designaciones de FTO, se volverán cada vez más violentos y radicales, lo que podría tener implicaciones para las empresas de todo el mundo. — Presión estadounidense sobre gobiernos extranjeros para que cumplan con las designaciones de FTO y combatan la actividad criminal interna de grupos de izquierdas, lo que ha generado incertidumbre política en los países afectados.


NETHERLANDS
Amsterdam
Rotterdam
Hanover
Bielefeld
GERMANY
Essen
Dusseldorf
Cologne
Antwerp
Brussels
BELGIUM
Lille
London
English Channel
Frankfurt am Main
Mannheim
Luxembourg
Saarbrucken
Paris

Europa

5

El reclutamiento civil altera el panorama de amenazas en toda Europa

Los actores hostiles están aprovechando cada vez más a los civiles, tanto de forma inconsciente como deliberada, para avanzar en sus objetivos estratégicos en los estados europeos, alterando el perfil tradicional de los actores de amenaza y complicando la atribución y las medidas de protección para gobiernos y empresas. China ha sido acusada de utilizar a sus nacionales e individuos coaccionados para realizar espionaje contra sitios sensibles; Se informa que Rusia ha reclutado a individuos para llevar a cabo actos criminales como incendios provocados o para operar drones dirigidos a infraestructuras nacionales críticas (CNI), mientras que Irán ha sido acusado de emplear grupos del crimen organizado francés y sueco (OCGs) y de financiar a grupos pro-palestinos para promover sus intereses en el extranjero.

— El creciente uso de civiles por parte de actores amenazantes probablemente se debe a los esfuerzos para desmantelar las redes tradicionales de espionaje en Occidente en medio de crecientes tensiones geopolíticas, que probablemente persistirán hasta 2026 y más allá si las tensiones se mantienen elevadas.

— Esta tendencia probablemente llevará a un aumento del reconocimiento hostil, el sabotaje y los ataques dirigidos que serán cada vez más difíciles de detectar o prevenir para las autoridades, lo que requerirá capacidades de vigilancia reforzadas y medidas de protección, mientras que los métodos de reclutamiento remoto proporcionan seguridad operativa para los actores amenazantes.

— Aunque este enfoque complica la atribución, casi con toda seguridad intensificará las tensiones geopolíticas y aumentará la sospecha en los Estados occidentales hacia ciudadanos extranjeros de países adversarios. También existe una posibilidad realista de que esta sospecha se extienda a las empresas, que también son vulnerables a la coacción o explotación.

Escenario	Condición del escenario	Probabilidad evaluada
La vigilancia y contrainteligencia reforzadas reducen incidentes y mejoran la atribución. Se controla la desconfianza hacia los extranjeros y las operaciones o ataques son menos frecuentes.	Mejora	Altamente improbable (25%)
Los actores hostiles continúan utilizando civiles en los niveles actuales, con incidentes ocurriendo de forma esporádica pero manteniéndose manejables.	Línea base	Posible / Probable (25%)
Los actores hostiles explotan cada vez más a los civiles, lo que provoca un aumento de los ataques. La atribución se vuelve cada vez más difícil y las empresas se enfrentan a mayores riesgos operativos y de seguridad.	Empeora	Improbable (55%)

Recomendaciones

— Mejorar la detección de amenazas y los protocolos de seguridad en sitios sensibles, incluyendo medidas de ciberseguridad reforzadas, vigilancia, selección de empleados y controles de acceso.

— Implementar y mantener una formación integral del personal sobre ingeniería social, riesgos de coacción y reconocimiento de conductas sospechosas, promoviendo al tiempo canales claros de reporte para posibles amenazas internas.

— Monitorizar las actividades estatales adversariales y las tácticas emergentes de reclutamiento, incluidas campañas de propaganda, y mantenerse actualizado sobre los requisitos regulatorios y de cumplimiento relacionados con amenazas dirigidas a civiles.

Indicadores	Implicaciones
— Aumento de incidentes de sabotaje / espionaje dirigidos a sitios sensibles gubernamentales o empresariales. — Aumento de ataques dirigidos contra comunidades disidentes / comunidades consideradas hostiles a los estados adversarios. — El contenido en línea se dirige cada vez más a civiles con propaganda y reclutamiento, especialmente en plataformas encriptadas. — Aumento de arrestos civiles con evidencia reportada de vínculos con actores estatales, incluidos aquellos sin motivación ideológica. — Un aumento en los ataques de baja sofisticación, incluyendo el uso incrementado de tecnología de drones civiles fácilmente accesibles para interrumpir infraestructuras críticas o realizar reconocimientos hostiles.	— Las interrupciones en infraestructuras críticas, cadenas de suministro y continuidad del negocio se vuelven más frecuentes y difíciles de prevenir. — Las empresas se enfrentan a mayores costes de seguridad y cumplimiento y a una mayor amenaza de incidentes internos. — Los riesgos reputacionales aumentan debido a filtraciones de información sensible y a la percepción de una seguridad débil. — El aumento de las tensiones tras incidentes entre estados interrumpe los lazos económicos y conduce a medidas contra empresas extranjeras de países adversarios, dificultando sus operaciones y el acceso al mercado.

El sentimiento antinmigración aumentan en toda Europa

El aumento de los niveles de migración irregular en Europa ha provocado una fuerte reacción pública, alimentando un sentimiento antinmigrante más fuerte en toda la región, una tendencia que probablemente se intensificará durante 2026. Este cambio ha ido acompañado de un aumento en la retórica de derechas, con muchos grupos de derechas que presentan el aumento de la migración como un tema político central. Como resultado, varios gobiernos europeos están adoptando políticas destinadas a abordar la migración irregular, fragmentando aún más tanto la opinión pública como el discurso político.

- Es probable que los grupos de derechas o de extrema derecha sigan organizando protestas para presionar a los gobiernos europeos a abordar la migración irregular, especialmente si las cifras migratorias siguen aumentando.
- El aumento de la polarización política y el auge de los medios alternativos probablemente aumentarán la posibilidad de que grupos opuestos participen en acciones hostiles. Es probable que las protestas organizadas den lugar a contramanifestaciones, incrementando el riesgo de enfrentamientos entre grupos opuestos o con las fuerzas de seguridad.
- Las protestas antiinmigración seguirán siendo promovidas y asistidas por figuras de alto perfil, lo que impulsará un aumento de la asistencia. y es probable que ganen un impulso adicional en respuesta a incidentes que supuestamente involucran a migrantes, especialmente cuando estos delitos son de naturaleza violenta o sexual. Estas tensiones pueden avivarse por actos de desorden informativo por parte de estados-nación hostiles y grupos de actores amenazantes.

Escenario	Condición del escenario	Probabilidad evaluada
La frecuencia e intensidad de la violencia y los disturbios relacionados con la migración disminuyen a medida que los gobiernos abordan las preocupaciones asociadas.	Mejora	Altamente improbable (15%)
Las protestas y disturbios antiinmigración continúan intensificándose en toda Europa, con presuntas actividades delictivas asociadas a migrantes que actúan como puntos de conflicto para manifestaciones de alto perfil.	Línea base	Posible / Probable (45%)
Aumento de la retórica violenta tras crímenes de alto perfil que involucran a migrantes, lo que llevó a grupos antiinmigración a formar redes más formales y sofisticadas coordinar acciones conjuntas.	Empeora	Improbable (40%)

Recomendaciones

- Mantener monitoreo sobre protestas planificadas en las inmediaciones de los activos de la organización y desarrollar planes de respuesta para gestionar distintos escenarios, incluyendo el refuerzo de medidas de seguridad en sitio y la implementación de estrategias para minimizar disrupciones operativas.
- Coordinar con las autoridades locales cuando se anticipen manifestaciones de gran magnitud cerca de activos empresariales.
- Evitar mensajes públicos que asocien a la organización con posiciones políticas, en particular aquellas relacionadas con migración.
- Mantener seguimiento del calendario político y del potencial de que se presenten episodios de agitación o disturbios como resultado de este.

Indicadores

- Aumento del panorama de protestas en los estados europeos afectados por el aumento de la migración irregular, influenciado por sentimientos antinmigración.
- Los intentos de reformar los controles fronterizos y las políticas relacionadas con el asilo no logran disuadir el ingreso a Europa de grandes flujos de migrantes irregulares.
- Los grupos de derecha / extrema derecha continúan ganando apoyo electoral, impulsados en parte por su postura firme sobre la migración irregular.
- Los gobiernos introducen políticas y regulaciones, incluidas restricciones a las protestas y castigos más severos, para frenar acciones disruptivas y perjudiciales.

Implicaciones

- Las protestas a gran escala y los enfrentamientos con las fuerzas de seguridad probablemente interrumpirán las rutas de transporte, la movilidad de los empleados y las cadenas de suministro.
- Las manifestaciones cerca de las operaciones de una organización probablemente aumenten el riesgo de exposición incidental a la violencia o daños a la propiedad.
- Los empleados de origen migrante se enfrentan a riesgos potenciales de seguridad, acoso o discriminación en o alrededor de las zonas afectadas por protestas.
- El aumento de las tensiones sociales probablemente complicará la implicación de las partes interesadas en las organizaciones europeas, especialmente en sectores políticamente sensibles.

Gobiernos europeos bajo presión financiera en medio de la transición económica

Numerosos países europeos se enfrentan a una creciente presión fiscal como resultado del alto gasto estatal, las tendencias demográficas y los desafíos geopolíticos y geoeconómicos, lo que supone un riesgo para las perspectivas económicas a largo plazo y la cohesión social de la región. Las tensiones políticas y económicas entre los países europeos y China, junto con los planes anunciados para desvincularse aún más de los recursos naturales rusos y otras tendencias emergentes como el aumento de las políticas económicas proteccionistas y la errática política económica de Estados Unidos, hacen que esta tendencia probablemente se extienda hasta 2026 y más allá.

— Las medidas previstas para reducir el déficit fiscal y la deuda nacional de Francia han sido factores significativos de inestabilidad política y disturbios sociales a lo largo de 2025, con múltiples manifestaciones masivas y huelgas que involucraron a cientos de miles de participantes que tuvieron lugar durante septiembre y octubre. Es probable que la implementación de medidas de austeridad similares en otros países europeos actúe como un punto conflictivo de disturbios.

— La Comisión Europea está considerando emitir reformas individualizadas a los Estados miembros como parte de un plan para vincular las reformas de las pensiones a la financiación central en el presupuesto de 2028, con el fin de reducir el riesgo fiscal que supone el envejecimiento de la población del bloque, según informes del 17 de octubre.

— Los Estados miembros de la UE deben presentar planes nacionales de diversificación, detallando cómo tienen la intención de eliminar las importaciones directas e indirectas de petróleo y gas rusos antes del 1 de marzo de 2026, mientras que otras sanciones entrarán en vigor a lo largo del año.

Escenario	Condición del escenario	Probabilidad evaluada
Los Estados europeos implementan reformas fiscales mientras las condiciones macroeconómicas mejoran, en línea con una reducción de la incertidumbre y la competencia geopolítica.	Mejora	Altamente improbable (10%)
Los Estados adoptan medidas para reducir los déficits fiscales; sin embargo, las condiciones macroeconómicas y geopolíticas agravan las presiones fiscales, generando desafíos políticos y agitación social.	Línea base	Posible / Probable (55%)
Los países europeos no logran implementar reformas fiscales, y las condiciones económicas continúan deteriorándose como consecuencia de la evolución del contexto geopolítico.	Empeora	Improbable (35%)

Recomendaciones

— Evaluar la probabilidad de que las operaciones empresariales actuales, contratos o asociaciones se vean afectados negativamente por medidas de austeridad planificadas o futuras, y evaluar su exposición.

— Integrar indicadores macroeconómicos y geopolíticos en la monitorización periódica de riesgos y monitorizar proactivamente para identificar señales de inestabilidad impulsadas por interrupciones en la cadena de suministro y cambios en las políticas.

— Diversificar las cadenas de suministro hacia jurisdicciones legales más estables e incorporar métricas de ASG, políticas y crediticias en la selección y supervisión de proveedores.

Indicadores	Implicaciones
— La UE instruyendo a los estados miembros a tomar medidas adicionales contra los déficits fiscales y los altos niveles de deuda nacional. — Países que adoptan medidas de reducción del déficit financiero, como cambios en la edad de jubilación, recortes en programas de bienestar social y degradación de los programas de pensiones. — La relación económica entre los países europeos y Estados Unidos se deteriora con poco tiempo, probablemente como resultado de una disputa política. — Países que no aprueban presupuestos anuales. — China anuncia nuevas investigaciones relacionadas con industrias asociadas al comercio europeo o contra importadores europeos específicos.	— Las condiciones económicas casi con toda seguridad tendrán una influencia significativa en el panorama político de la región, con el deterioro que fomentará el apoyo a partidos radicales o marginales. — Las medidas de austeridad y otras reformas fiscales moldean el panorama empresarial de la región y afectan a la planificación a largo plazo — Protestas sindicales cada vez más frecuentes o potencialmente intensas en países de toda la región. — Mayor probabilidad de despidos masivos y pérdidas de empleos en diversos sectores.

Comodines

Mercados globales desestabilizados por el estallido de la burbuja de la IA

La creciente valoración de las empresas vinculadas a la Inteligencia Artificial (IA) ha generado preocupaciones sobre una posible burbuja en la industria, con numerosos analistas estableciendo paralelismos con la burbuja puntocom que surgió alrededor del cambio de milenio y que derivó en un crash bursátil severo.

Las denominadas “Magnificent Seven”, es decir, Alphabet, Amazon, Apple, Meta, Microsoft, Nvidia y Tesla, presentan una capitalización de mercado combinada de aproximadamente 21,5 billones de dólares, representando cerca del 35 % de la capitalización total del mercado a noviembre de 2025. A pesar de estas preocupaciones, estas compañías continúan recibiendo crecientes inversiones, impulsadas principalmente por el incremento en productividad y el potencial de crecimiento económico proyectado que promete la tecnología de IA.

— Nvidia, un actor clave, tiene una valoración de mercado de aproximadamente 5 billones de dólares, superior al PIB de Japón, lo que implica que pequeñas variaciones en su valoración, provocadas por eventos como resultados financieros por debajo de lo esperado o cambios regulatorios, pueden generar oscilaciones significativas en los mercados globales.

— Los inversores han señalado que muchas empresas ‘hiperescala’ reparten el costo de las unidades de procesamiento gráfico (GPU) durante cinco o seis años, a pesar de que Nvidia ha lanzado nuevas arquitecturas que deprecian el valor de generaciones anteriores mucho más rápido, en una práctica descrita como una de “las estafas más comunes de la era moderna”

— La valoración del sector ha sido impulsada en parte por compromisos de gasto asumidos por varias empresas que son significativamente superiores a sus ingresos anuales actuales. Los ingresos de OpenAI se estiman en ~20.000 millones de dólares en 2025, pero se ha comprometido a invertir ~1,4 billones en empresas como AWS, Microsoft y Oracle entre 2025 y 2032.

Escenario	Condición del escenario	Probabilidad evaluada
Las organizaciones ralentizan el endeudamiento para financiar el desarrollo de la IA, lo que resulta en una capitalización bursátil menos concentrada, menor volatilidad en torno a la influencia de la IA y ayudando a evitar un ‘estallido’ de burbujas.	Mejora	Altamente improbable (15%)
La burbuja especulativa sigue creciendo y agrava la presión sobre los mercados financieros, lo que resulta en más riesgo, volatilidad e incertidumbre.	Línea base	Posible / Probable (40%)
La valoración de las empresas asociadas a la IA sigue creciendo sin ningún gran impacto avances tecnológicos o aumento significativo de las fuentes de ingresos, lo que llevó a un eventual desplome del mercado.	Empeora	Improbable (40%)

Recomendaciones

— Mejorar las habilidades de la fuerza laboral para mitigar la volatilidad del mercado y garantizar la resiliencia a largo plazo desarrollando habilidades humanas como el razonamiento ético y la resolución de problemas complejos.

— Diversificar carteras de activos con otras tecnologías centradas en mejorar las capacidades operativas, mitigar el impacto operativo de la pérdida de acceso o aumentos significativos de costes para la capacidad de IA.

— Mantener la conciencia de las señales fluctuantes del mercado de IA y de los cambios regulatorios financieros para informar planes de contingencia que mitiguen la amenaza de colapso.

Indicadores	Implicaciones
— Se observó una disminución de la confianza entre las organizaciones tecnológicas y los inversores. — Las valoraciones siguen subiendo y dan lugar a un nuevo mercado sostenido centrado en la tecnología. — Las organizaciones de los 'Siete Magníficos' no cumplen con los objetivos de beneficios y ventas, aumentando la volatilidad del mercado. — Las organizaciones asociadas a la IA realizan despidos masivos o adoptan otras medidas de reducción de costes. — Las condiciones económicas empeoran, resultando en tipos de interés más altos. — Las organizaciones solicitan a los gobiernos un rescate económico o protección para garantizar su sostenibilidad.	— La recesión económica afecta negativamente al producto interior bruto (PIB), las tasas de empleo, el nivel de vida y los planes de ahorro. — El desarrollo tecnológico futuro se retrasará debido a una posible pérdida generalizada de confianza en tecnologías sofisticadas. — El malestar público derivado de un aumento de sentimientos en contra de la IA y el sector financiero. — Endurecimiento de la regulación financiera impulsada por la presión política y pública para evitar futuros colapsos.

Aumento de la competencia geopolítica en la región ártica

La competencia por el control del acceso a recursos, rutas marítimas y territorios estratégicos en el Ártico está aumentando, ya que el deshielo provocado por el calentamiento global hace que la región sea más accesible. Esto ha provocado una mayor militarización del Ártico y un aumento de las tensiones entre países rivales. Las tensiones globales más amplias especialmente entre Rusia, Estados Unidos y países del norte de Europa— probablemente acelerarán la carrera por reclamar y controlarb rutas y ubicaciones clave en la región en 2026.

— Potencias globales, como Rusia y Estados Unidos, compiten cada vez más por el control del Ártico, principalmente invirtiendo en tecnologías destinadas a mejorar el acceso regional y la influencia de proyectos, como los rompehielos, con ambos países buscando ampliar el acceso y el uso de nuevas rutas marítimas potenciales.

— Los miembros de la OTAN están realizando ejercicios militares conjuntos en el Ártico con creciente frecuencia, mientras que aquellos con territorio ártico, como los países nórdicos, han desarrollado alianzas con miembros que carecen de territorio ártico para reforzar la seguridad en respuesta a los esfuerzos rusos por desarrollar presencia militar en la región.

— Se informa que las disputas territoriales, principalmente sobre áreas que se cree albergan minerales críticos y otros recursos naturales, se están priorizando por encima de las preocupaciones de las poblaciones indígenas, lo que subraya la ineficacia de instituciones regionales, como el Consejo Ártico, respecto a su capacidad para proteger los derechos de los habitantes de la región.

Escenario	Condición del escenario	Probabilidad evaluada
Los esfuerzos por identificar rutas marítimas viables no tienen éxito o se consideran inviables, lo que disminuye el interés en el Ártico. Los países con intereses en la región identifican vías de cooperación, como a través de acuerdos sobre límites a la presencia militar o industrial.	Mejora	Altamente improbable (10%)
La militarización del Ártico sigue aumentando de forma constante, mientras que las acciones rusas de guerra en zona gris (GZW) se vuelven más frecuentes. La competencia por el territorio está impulsada por el descubrimiento de grandes reservas de recursos naturales o ubicaciones estratégicamente significativas.	Línea base	Posible / Probable (65%)
Rusia reduce el enfoque en Ucrania (ya sea por alto el fuego o por un cambio de estrategia), cambiando esfuerzos hacia aumentar su influencia en la región ártica, aumentando el riesgo de confrontación militar.	Empeora	Improbable (25%)

Recomendaciones

— Se recomienda a las empresas con intereses en las regiones árticas o nórdicas — incluidas las cadenas de suministro como rutas marítimas— que mantengan la atención sobre los desarrollos geopolíticos en la región.

— Preparar planes de contingencia debido al potencial de enfrentamientos armados y disputas militares en el Ártico, incluyendo el cierre o restricción de rutas comerciales clave.

— Las organizaciones vinculadas a operaciones relacionadas con el interés y desarrollo global en los territorios árticos deberían evaluar el potencial de represalias y los impactos negativos en la reputación asociados a las críticas de las poblaciones indígenas.

Indicadores	Implicaciones
— Organismos científicos y estudios creíbles indican que el deshielo del hielo ártico continúa o aumenta. — Países y alianzas con intereses en la región ártica compran o construyen activos que probablemente se utilicen para expandir o consolidar su presencia (como los rompehielos). — Los ejercicios militares de la OTAN y Rusia en el Ártico aumentan en frecuencia y escala. — Las acciones GZW rusas dirigidas a competidores regionales aumentan en frecuencia y complejidad. — Las comunidades indígenas en el Ártico intensifican los esfuerzos para concienciar sobre sus quejas y protestar contra las acciones de los competidores regionales.	— Las organizaciones que operan en el Ártico, especialmente aquellas en industrias estratégicas, probablemente estarán en riesgo de ser atacadas por acciones de amenaza como el sabotaje. — Las disputas legales sobre territorios disputados probablemente supondrán desafíos para las empresasque operan en la región. — Las organizaciones con intereses en el Ártico se convierten en objetivos de activismo relacionado con las poblaciones indígenas. — La militarización y las posibles escaladas probablemente incitarán preocupaciones de inversores y desinversión en ciertos activos árticos. — La mejora de la infraestructura a lo largo de las rutas marítimas árticas probablemente fortalecerá las cadenas de suministro dependientes.

El dominio espacial eleva la amenaza para la seguridad nacional y los sectores privados

La creciente dependencia de la tecnología espacial — y los esfuerzos asociados de los estados nación para ejercer influencia y control sobre el espacio— probablemente acelerará las amenazas de seguridad nacional y comerciales en 2026. Rusia, China y Estados Unidos avanzaron notablemente en capacidades militares basadas en el espacio en 2025, incluyendo sistemas antisatélite (ASAT) y despliegues de contramisiles. Aunque la arquitectura de armas basadas en el espacio es una aspiración a largo plazo, la amenaza de impactos en las redes de comunicaciones y geolocalización tanto por fenómenos naturales como por intervención humana, como la guerra en zonas grises (GZW) que ataca satélites, probablemente seguirá aumentando.

- Los satélites comerciales probablemente tendrán un papel en la planificación militar y de GZW, arriesgando interrupciones en sistemas que proporcionan servicios clave como comunicaciones, imágenes satelitales y servicios de navegación / geolocalización.
- Además, la creciente dependencia de tecnologías altamente sensibles expondrá casi con toda seguridad a las organizaciones al riesgo de impactos asociados a fenómenos como la radiación solar, incluyendo cortes y daños en el sistema. El próximo máximo solar, previsto para principios de 2026, servirá como posible desencadenante de erupciones solares y eyección de masa coronal, que a su vez aumentan el riesgo de inactividad en infraestructuras clave de energía y comunicaciones.
- Un acuerdo internacional que regule el desarrollo de tecnología militar o potencialmente hostil basada en el espacio es poco probable, lo que aumenta el riesgo de una 'carrera armamentística' espacial y amenazas asociadas como acciones de GZW.

Escenario	Condición del escenario	Probabilidad evaluada
Las grandes potencias desarrollan un diálogo vinculante sobre la limitación de la capacidad ofensiva espacial, mientras que el máximo solar de 2026 pasa con impactos mínimos.	Mejora	Altamente improbable (10%)
Las naciones continúan proliferando capacidades espaciales, empleando GZW en intentos de interrumpir el CNI, mientras que la radiación solar contribuye a eventos disruptivos aislados.	Línea base	Posible / Probable (70%)
Se produce un evento de fallo global o masivo de infraestructura debido a una gran pérdida de satélites capacidad, ya sea por intervención militar directa, acciones GZW o espacio extremo Eventos meteorológicos.	Empeora	Improbable (10%)

Recomendaciones

- Evaluar la exposición a impactos asociados a la pérdida de sistemas dependientes de la tecnología satelital, en particular conectividad (tanto telefonía como internet), geolocalización y seguimiento, e imágenes.
- Revisar cualquier dependencia de equipos sensibles a picos de radiación solar y los impactos asociados a tiempos de inactividad o daños a los anteriores.
- Considerar realizar ejercicios de simulación o 'wargaming' para escenarios como una gran tormenta geomagnética y sus impactos asociados.

Indicadores

- La Fuerza Espacial de EE. UU. operacionaliza los sistemas de combate según lo previsto; China y Rusia despliegan herramientas ASAT espaciales y terrestres.
- Crecientes tensiones geopolíticas sobre el despliegue o desarrollo de tecnologías espaciales (incluidas las armas).
- Incrementos en las interrupciones reportadas por servicios que dependen de tecnología satelital.
- Los terminales terrestres asociados con la funcionalidad del satélite informan de un aumento de intentos de intrusión cibernética.
- La actividad de pulsos solares ocurre en línea con eventos solares máximos anteriores, incluyendo varias llamaradas solares de eyecciones de masa coronal.

Implicaciones

- Las interrupciones en los sistemas de navegación / GPS provocan retrasos en el envío y el transporte.
- Las fallas en los sistemas digitales pueden detener las transferencias de pagos globales, generando incertidumbre financiera.
- La pérdida de acceso a satélites conectados a infraestructuras nacionales críticas (CNI) degrada gravemente los servicios de emergencia y las telecomunicaciones.
- La interrupción de la vigilancia permite operaciones militares, empeorando la seguridad regional.
- Los sistemas de alerta temprana para fenómenos meteorológicos severos y desastres naturales se vuelven ineficaces, dificultando la evacuación y la planificación de continuidad.

Puntos críticos y fechas importantes

2026 Puntos críticos y fechas importantes

AMEA

JAN

- **1 Enero:** día de la República de Taiwán
- **3 Enero:** aniversario del
- asesinato de Qasem Soleimani
- **14 Enero:** aniversario de la Revolución tunecina —
- **15 Enero:** aniversario de la Ataque terrorista de Ra'anana en 2024
- **25 Enero:** aniversario de la Revolución Egipcia de 2011

FEB

- **1 Febrero:** aniversario del golpe militar de Myanmar de 2021
- **11 Febrero:** día de la Revolución Islámica (Irán)
- 14 Febrero: aniversario del levantamiento de Baréin de 2011
- **15 Febrero:** día de la 1 Liberación de Afganistán
- **15 Febrero:** aniversario de la Revolución Libia de 2011
- **20 Febrero:** aniversario de las protestas por la reforma marroquí de 2011

MAR

- **5 Marzo:** elecciones generales nepalíes
- **15 Marzo:** aniversario del tiroteo en la mezquita de Christchurch en 2019
- **17 Marzo:** día de San Patricio
- **28 Marzo:** día de Al Quds
- **30 Marzo:** Eid al-Fitr

APR

- **1-9 Abril:** Pascua
- **5 Abril:** domingo de Pascua
- **14 Abril:** Yom HaShoah

MAY

- **1 Mayo:** primero de mayo
- **7 - 10 Mayo:** aniversario del conflicto India-Pakistán
- **15 Mayo:** día de Al Nakba
- **25 Mayo:** día de Jerusalén

JUN

- **1 Junio:** elecciones generales etíopes
- **4 Junio:** aniversario de la masacre de la Plaza de Tiananmen de 1989
- **4 Junio:** peregrinación del Hajj
- **3-24 Junio:** aniversario del conflicto Irán-Israel
- **26 Junio:** Ashura

JUL

— **24-28 Julio:** aniversario de la disputa fronteriza Camboya-Tailandia

AUG

— **14 Agosto:** día de la independencia de Pakistán
— **15 Agosto:** día de la independencia de la India

SEP

— **21 Septiembre:** Yom Kippur
— **25 Septiembre:** Sukkot

OCT

— **7 Octubre:** tercer aniversario de la escalada del conflicto entre Gaza e Israel
— **9-19 Octubre:** aniversario del conflicto Afganistán-Pakistán
— **14 Octubre:** aniversario del golpe de Estado malgache

NOV

— **2 Noviembre:** día de Balfour
— **8 Noviembre:** Diwali
— **30 Noviembre:** elecciones parliamentarias kirguisas

DEC

— **5 Diciembre:** elecciones presidenciales de Gambia
— **5-12 Diciembre:** Janucá
— **11 Diciembre:** aniversario de la Resolución 194 de la Asamblea General de la ONU de 1948
— **22 Diciembre:** Sudán del Sur celebra sus primeras elecciones generales
— **25 Diciembre:** Navidad
— **31 Diciembre:** Nochevieja

2026 Puntos críticos y fechas importantes

América

JAN

- **1 Enero:** Año Nuevo
- **6 Enero:** aniversario de la insurrección en el Capitolio de EE. UU.
- **7 Enero:** aniversario de la masacre de Juliaca
- **11-17 de enero:** semana de Al-Aqsa
- **27 Enero:** día de los conmemorativos del Holocausto
- **27 Enero:** Isra y Miraj

FEB

- **4 Febrero:** aniversario del intento de golpe de estado en Venezuela de 1992
- **13-14 Febrero:** Shab-e-Barat
- **13-18 Febrero:** carnaval de Rio
- **14 Febrero:** aniversario del tiroteo en el desfile de Kansas City en 2024
- **17 Febrero:** día de los presidentes de EE. UU.
- **26 Febrero:** Maha Shivrati

MAR

- **17 Marzo:** día de San Patricio
- **28 Marzo:** día de Al Quds
- **30 Marzo:** Eid al-Fitr

APR

- **1-9 Abril:** Pascua
- **5 Abril:** domingo de Pascua
- **12 Abril:** elecciones generales peruanas

MAY

- **1 Mayo:** primero de mayo
- **5 Mayo:** cinco de Mayo
- **15 Mayo:** día de Al Nakba

JUN

- **26 Junio:** Ashura

JUL

— **4 Julio:** día de la independencia de EE. UU.

AUG

— **6 Agosto:** día de la independencia de Bolivia
— **30 Agosto:** Elecciones generales de Haití

SEP

— **10 Septiembre:** primer aniversario del asesinato de Charlie Kirk
— **20-27 Septiembre:** Climate Week NYC 2026

OCT

— **4 Octubre:** elecciones generales brasileñas
— **7 Octubre:** tercer aniversario de la escalada del conflicto entre Gaza e Israel

NOV

— **2 Noviembre:** día de Balfour
— **3 Noviembre:** elecciones de mitad de mandato EE. UU.
— **8 Noviembre:** Diwali

DEC

— **5-12 Diciembre:** Janucá
— **11 Diciembre:** aniversario de la Resolución 194 de la Asamblea General de la ONU de 1948
— **25 Diciembre:** Navidad
— **31 Diciembre:** Nochevieja

2026 Puntos de conflicto y fechas importantes

Europa

JAN

- **1 Enero:** Año nuevo
- **7 Enero**: aniversario del ataque terrorista de Charlie Hebdo en 2015
- **19-23 Enero:** Foro Económico Mundial
- **11-17 Enero:** semana de Al-Aqsa
- **27 Enero:** día de la conmemoración en memoria de las víctimas del Holocausto
- **27 Enero:** Isra and Miraj

FEB

- **13 Febrero:** conferencia de seguridad de Múnich
- **13 Febrero:** aniversario del ataque de coche en Múnich de 2025
- **13-14 Febrero:** Shab-e-Barat
- **24 Febrero:** aniversario de la invasión rusa de Ucrania en 2022
- **28 Febrero:** aniversario del desastre ferroviario de Tempe

MAR

- **17 Marzo:** día de San Patricio
- **28 Marzo:** día de Al Quds
- **30 Marzo:** Eid al-Fitr

APR

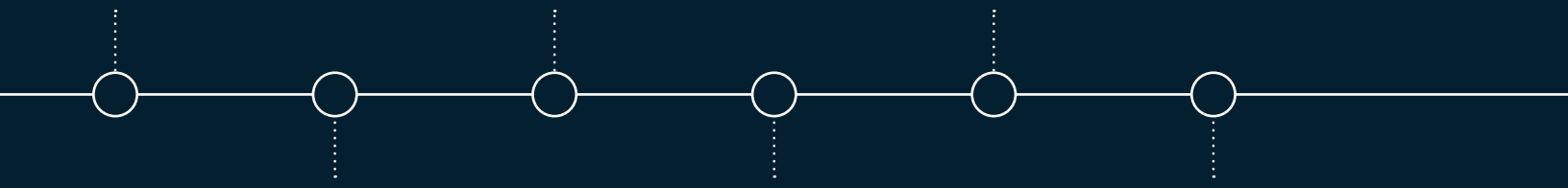
- **1-9 Abril:** Pascua
- **3 Abril:** elecciones parlamentarias húngaras
- **5 Abril:** domingo de Pascua

MAY

- **1 Mayo:** primero de mayo
- **9 Mayo:** día de la Victoria
- **15 Mayo:** día del Al Nakba

JUN

- **7 Junio:** elecciones generales armenias
- **26 Junio:** Ashura



JUL

— **14 Julio:** día de la Bastilla

AUG

— **24 Agosto:** día de la Independencia de Ucrania

SEP

— **13 Septiembre:** elecciones generales suecas

OCT

— **3 Octubre:** elecciones parlamentarias de Letonia
— **7 Octubre:** tercer aniversario de la escalada del conflicto entre Gaza e Israel

NOV

— **2 Noviembre:** día de Balfour
— **8 Noviembre:** Diwali

DEC

— **5-12 Diciembre:** Janucá
— **11 Diciembre:** aniversario de la Resolución 194 de la Asamblea General de la ONU de 1948
— **25 Diciembre:** Navidad
— **31 Diciembre:** Nochevieja

Contáctanos

intelligence@securitas.com